SECTION C – PERFORMANCE WORK STATEMENT (PWS)

C.1. PURPOSE

The purpose of this Task Order is to provide communications and information technology (IT) services to support U.S. Africa Command (AFRICOM), U.S. European Command (EUCOM), Combined Joint Task Force - Horn of Africa (CJTF-HOA), and associated staff elements and organizations. All parties require devices, hardware, software, and network IT and communications support services for the continued enhancement, operation, maintenance, and life cycle support for networks, office automation, communications, and software and systems applications supporting C4 systems.

C.2. BACKGROUND

The stakeholder organizations supported under this Task Order are defined below. PWS section C.2 and attachments appended to this PWS provide further information about the organizational and technical "footprints" covered under the scope as well as information about the Government oversight structure applicable to the administration and management of this Task Order.

C.2.1. ORGANIZATIONS

C.2.1.1. 5th SIGNAL COMMAND (5SC)

The 5th Signal Command (5SC) is the European-based tactical and strategic communications organization of the United States Army specializing in command and control which supports theater-limited, joint-forces, and combined forces activities. The command's mission statement specifies that it will: *"build, operate, defend, and extend network capabilities in order to enable mission command and create tactical, operational and strategic flexibility for Army, Joint and Multi-National Forces within the EUCOM and AFRICOM Areas of Operations."*

As the IT Service Provider within the AFRICOM and EUCOM AORs ---

- 5SC has assumed responsibility for providing IT services to AFRICOM and accomplishes this mission through a combination of Active Duty, Department of the Army Civilian, and Contractor solutions. *Note: 5SC responsibilities for AFRICOM encompass services to the Horn of Africa (HOA) region, as the networks and information systems used in HOA are an extension of the AFRICOM IT enterprise.*
- A decision made in December 2013 calls for the 5th Signal Command to assume IT Service Provider responsibilities for EUCOM and a transition is underway in which the day-to-day service responsibilities are migrating under 5SC and plans to move the EUCOM security stack to the JRSS . As migration activities continue, the Government anticipates the need for the Contractor performing work under this Task Order to evolve services, techniques, processes, and procedures i.a.w with the Government's changing needs.

5SC provides technical direction and contract oversight for the IT services provided to AFRICOM, EUCOM, and CJTF-HOA as well as other HOA regional end users requiring services under this Task Order.

As 5SC IT service provider responsibilities within the theater evolve and the Joint Information Environment (JIE) initiative further matures, the Government anticipates that the services delivered by the contractor performing under this Task Order may be impacted by Government driven change. Adoption of new/revised government-government service level agreements (SLAs); and changes in processes, required quality of services, requisite performance standards, operational/programmatic needs, or other factors may impact (increase or decrease) the level of contract support required, thereby resulting in the need to scale contractor resources up or down in various operational areas to meet mission demands. At Task Order start, it is not possible to fully predict in advance what operational-level changes may occur, nor to anticipate the extent to which functions or services under this Task Order may be affected by such change. The service desk and incident management processes in particular are areas expected to be affected by how 5SC manages these responsibilities today vice in the future. Other areas could follow suit. It is expected that contractor flexibility in adapting to and positively influencing such Government driven change is a necessity for successful Task Order performance.

C.2.1.2. U.S. AFRICA COMMAND (AFRICOM)

HQ U.S. Africa Command (AFRICOM) is the geographic combatant command headquarters for the area of responsibility (AOR) covering Africa and the African Theater of Operations. It is currently headquartered at Kelley Barracks, Stuttgart, Germany.

The AFRICOM Command, Control, Communications and Computers (C4) Systems Directorate (C4S) currently provides theater-level policy, planning, and implementation oversight for C4 systems within the Areas of Responsibility (AOR). The C4S provides the policy, plans, programs, and systems support to shape the C4 environment, ensuring information dominance, and interoperable C4 systems, to prevent conflict, respond in crisis, prepare for combat, and if required, fight to win.

C.2.1.3. U.S.EUROPEAN COMMAND (EUCOM)

HQ U.S. European Command (EUCOM) is the geographic combatant command headquarters for the AOR covering Europe and the European Theater of Operations.

The EUCOM Command, Control, Communications and Computers/Cyber Directorate (ECJ6) currently provides theater-level policy, planning, and implementation oversight for C4 systems within the Areas of Responsibility (AOR). The ECJ6 provides the policy, plans, programs, and systems support to shape the C3 environment, ensuring information dominance, and interoperable C3 systems, to prevent conflict, respond in crisis, prepare for combat, and if required, fight to win.

Although 5SC is designated as the IT Service Provider for EUCOM, there are eight mission-specific areas that EUCOM has retained oversight of:

MNIS	C2 (JOC/EMCC)	KM	Threat Assessment
GCCS	Web Services	TCSMIS	Office of Defense Cooperation

C.2.1.4. COMBINED JOINT TASK FORCE – HORN OF AFRICA (CJTF-HOA)

The Combined Joint Task Force Horn of Africa supports partner nation military operations in East Africa to defeat violent extremist organizations, conducts focused military-to-military engagement to strengthen East African partner nation militaries, and conducts crisis response and personnel recovery in support of U.S. military, diplomatic, and civilian personnel throughout East Africa in order to protect and defend the national security interests of the United States.

CJTF-HOA is located at Camp Lemonnier, Djibouti City, Djibouti

5th Signal Command through the Joint IT Service Management Office – Horn of Africa (JITSMO-HOA) has responsibility to provide a wide range of joint services end points that include data, voice, and video users on Camp Lemonnier as well as interfacing to other Combatant Commands (COCOMs) and DoD communications environments.

C.2.2. CAPABILITIES DELIVERED BY THE EUCOM/AFRICOM NETWORKS

The current AFRICOM and EUCOM networks have been deliberately implemented with a balance between technology and cost. Emerging technologies are actively monitored for potential incorporation into the existing architecture. As a result of careful technology consideration the COCOMs have built and maintained stable, well-structured networks.

AFRICOM/EUCOM/CJTF HOA requires the following capabilities for the network:

- System Availability and Responsiveness.
- IT Service Management.
- Data Protection.
- Security.
- Adaptability.
- Collaboration.
- Cross-Domain Security and Information Exchange.
- System Interoperability.
- Redundancy.
- Survivability.
- Scalability.

The EUCOM/AFRICOM Networks will serve as the Combatant Command's (COCOM's) instantiation of the Global Information Grid (GIG) and will use DoD-provided enterprise services to the greatest extent feasible. The EUCOM/AFRICOM Networks will minimize the transition between current DoD networks and the future vision for the DoD/COCOM Network Environment.

The EUCOM/AFRICOM Networks will provide a set of core and enterprise applications and will serve as the COCOM's instantiation of an enterprise network to support unique applications. EUCOM/AFRICOM, along with DoD and Joint guidance, will define the methods in which future applications must be developed, and operate and establish rules for application hosting.

The EUCOM/AFRICOM Networks will leverage the Net-Centric Core Enterprise Services (NCES) to the fullest extent possible, including Enterprise Services Management, Discovery, Messaging, Collaboration, Mediation, Storage, Information Assurance (IA)/Security, Application, and User Assistant services. The EUCOM/AFRICOM Networks will have common services criteria established that go across the Internet, NIPRNET, and SIPRNET environments to include a standard credentialing validation and directory. The EUCOM/AFRICOM Networks will augment the GIG and NCES capabilities by guiding the transformation of the existing networks and legacy environments of applications, databases, networks, and facilities into an integrated enterprise information architecture capable of supporting Net-Centric Operations Warfare (NCOW). The EUCOM/AFRICOM Networks will provide terminal/seat, application, and data hosting services consistent with the common computing environment developed for DoD enterprise IT services.

The EUCOM/AFRICOM Networks will provide access to host-based applications as well as local client-server, web-based, and portal-based applications. The networks will provide access to four network environments Secure Internet Protocol Router Network (SIPRNET), Nonsecure Internet Protocol Router

Network (NIPRNET), Coalition Network(s), and Internet consistent with DoD security guidelines. The certification and accreditation of these four environments has been completed. The AFRICOM/EUCOM Networks may be employed on a desktop alongside another hybrid client providing special functionality, including multi-level security. While hardware maintained under the scope of this Task Order will frequently be located in space where multi-level security systems reside; the maintenance and support of such multi-level security systems is provided by separate support contractors. This Task Order does <u>not</u> include any requirements/plans to implement or support multi-level security systems on behalf of J6/C4 Systems.

Data hosting for joint supported applications will be provided through a mix of data centers structured to provide reliable, responsive access to data and information for the COCOM's warfighting and business communities. These data centers will provide application and data hosting as well as support application Continuity of Operations (COOP) requirements.

C.2.2.1. SYSTEM CAPABILITIES

Warfighters and business processes depend critically on assured and high quality communications, IT, and networking performance. The EUCOM and AFRICOM networks will support the warfighter and business communities by providing:

- Network services.
- Communications services.
- Video and presentation services
- Information assurance.
- Customer service and responsiveness.
- Leveraging of DoD Enterprise services.
- Domain architecture, engineering and installation.
- Governance.

Challenges and risks the Government current faces in delivering such capabilities to their customer base include:

- Responding to unforecasted change;
- Addressing challenges that arise with routine operations;
- Managing unknowns and emerging/changing requirements in light of uncertainties associated with the JIE initiatives

Communications and IT systems capabilities for EUCOM/AFRICOM are best served by tiered requirements and associated threshold and objective criteria in terms of critical and non-critical services/capabilities. The following terms and definitions apply.

- <u>Critical Services</u> are defined as those services that when unavailable or inaccessible prevent the system from performing one or more mission critical functions. They also include any service required by another application to fulfill its mission critical functions. This includes all aspects of that service including all required supporting services and access to the service with the exception of the user access device. A Critical Service is considered down when it is unavailable or inaccessible.

- <u>Non-Critical Services</u> are defined as all services not identified as Critical Services. They include all aspects of that service including all required supporting services and access to the service with the exception of the user access device. A Non-Critical Service is considered down when it is unavailable or inaccessible.

- Critical user access devices are those devices with which users must access Critical Services during the normal execution of their jobs. A critical user access device is considered down when the operator is unable use the Critical Services required during the normal execution of his/her job when the service is available and accessible.

- Non-critical user access devices are defined as all user access devices not identified as Critical Services. These devices are considered down when the operator cannot use any service from that device and at least one service is available and accessible.

- Disaster Recovery (DR) is the processes, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.

- COOP involves establishing and implementing plans for emergency response, storage and backup operations, off-site storage, and post-disaster recovery of information systems.

- Business Continuity Planning is an interdisciplinary concept used to create and validate a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption.

C.2.2.2. SITES AND CUSTOMER BASE

Known sites and the customer base supported under the Task Order's current footprint are listed below. Additional site(s) and number of personnel included in the user base is anticipated to grow during the period of performance of this Task Order. The current footprint includes:

- Patch Barracks (Stuttgart, Germany) with approximately 2800 users (5000 seats spanning SIPR/NIPRnet.)
  - To include General Officer (GO)/(Flag Officer (FO)/Very Important Person (VIP) Quarters. The EUCOM VIP customer base consists of +/- 200 personnel which typically includes GO/FO/SES-level billets and their associated O-6 level staff.
- Kelley Barracks (Stuttgart, Germany) with approximately 50 EUCOM users and approximately 2200 AFRICOM users (4000 seats spanning SIPR/NIPRnet.)
  - To include GO/FO/VIP Quarters. The AFRICOM VIP customer base consists of +/- 200 personnel GO/FO/Ambassadors/SES-level billets and their associated O-6 level staff.
- Camp Lemonnier, Djibouti City, Djibouti with approximately 2500 users (4000 seats spanning SIPR/NIPRnet.)
  - To include VIPs and forward deployed users;
  - To include support for HOA Sites – both permanent and temporary, which change from time to time, dependent on mission needs. Currently there are 7 supported Forward Operating Locations within the Combined Joint Operations Area (CJOA), though this number may expand or contract from time-to time.
- Stuttgart Army Airfield (Stuttgart, Germany) with approximately 150 users.
- Supreme Headquarters, Allied Powers Europe (SHAPE) with approximately 200 users in Mons, Belgium.

- Pentagon with approximately 50 users (25 for each COCOM Liaison Office)
- RAF Molesworth, UK with approximately 500 AFRICOM and 700 EUCOM users
- Office of Defense Cooperation (ODCs) and other remote locations in EUCOM's AOR countries, mostly in or near U.S. Embassies.
- George C. Marshall Center (Garmisch, Germany) with approximately 20 remote users.

Other potential 5SC future sites include, but are not limited to: Wiesbaden, Kaiserslautern, GE.

Note: *Very Important Person (VIP) - VIPs include end users in key leadership and management positions with enhanced service desk and desk side support service requirements. VIPs are located at the COCOM HQ as well as other sites supported under the scope of this Task Order*

C.2.2.3. JOINT AND DOD-LEVEL CONSIDERATIONS

The EUCOM/AFRICOM Networks will have common services criteria established that go across the NIPR and SIPR environments to include a standard credentialing validation service and utilization of the Identity and Access Management (IdAM) and Identity Synchronization Service (IdSS). The EUCOM/AFRICOM Networks will augment the GIG and NCES capabilities by guiding the transformation of the existing and legacy environments of applications, databases, networks, and facilities into integrated enterprise information architecture capable of supporting Net-Centric Operations and Warfare (NCOW). The EUCOM/AFRICOM Networks will also provide transport and high assurance guards, as required, for the approved networks that will initially remain separate (for example: JWICS, Combined Enterprise Regional Information Exchange System (CENTRIXS), Global Command Control System Joint (GCCS-J), etc.).

The EUCOM/AFRICOM Networks Enterprise Services as a core capability of the EUCOM/AFRICOM Network environments shall be the COCOM's instrument for the deployment of net-centric infrastructure and fielding of interoperable enterprise capabilities. These capabilities will mutually support and contribute to the Department of Defense (DoD) overall Global Information Grid (GIG) Enterprise Services (GES), Net-Centric Enterprise Services (NCES) and Information Technology (IT) capabilities. The EUCOM/AFRICOM Networks shall deliver the enterprise IT infrastructure necessary for organizing and managing hardware, software and data as virtualized resources, hosting applications as services, using data sources, and offering NCES core services along with other core services as they become available. The infrastructure will support a Service Oriented Architecture (SOA) design methodology for connectivity between mission area processes and IT infrastructure using DoD and industry standard hardware and software building blocks. The overall intent of the EUCOM/AFRICOM Network Enterprise Services is to rationally transform the current infrastructure and management practices by implementing a disciplined enterprise approach to IT architecture, governance and investment in concert with joint and DoD level initiatives. This will improve the end-to-end process of how information is produced, organized, stored, protected, accessed, analyzed, collaborated, staffed and presented to users.

C.2.3. CURRENT COMMUNICATIONS AND IT NETWORK ENVIRONMENT

AFRICOM/EUCOM C4 systems include:

- Sensitive but Unclassified Wide Area Network (UWAN, also referred to as ULAN)
- Secret Wide/Local Area Network (SWAN, also referred to as SLAN)
- Coalition (to include bilateral) networks

- Visual information, presentation and collaboration systems (desktop VTC systems, conference room VTC facilities)
- IP-based Telephony and wireless
- Conference and exercise facilities
- Customer service help desk

[Note: The USAFRICOM network is commonly referred to as the Joint Enterprise Network (JEN)]

The AFRICOM C4 architecture has been separated from the EUCOM C4 infrastructure. The EUCOM/AFRICOM hardware infrastructure includes Intel-based PCs and Servers, Sun workstations and servers, printers and other devices connected to the network (e.g., digital senders). The EUCOM/AFRICOM Networks infrastructure includes fiber optic, coaxial, and twisted pair cabling. Network hardware includes components such as hubs, routers, and switches primarily from Cisco, Cabletron, and Bay Networks. Network operating systems currently in use include Windows 200X, and Oracle Solaris. The EUCOM/AFRICOM C4 networks rely heavily on commercial-off-the-shelf (COTS) and Government-off-the-shelf (GOTS) software for most applications. Database management systems include: SYBASE, Oracle, Access, and MS SQL. Office automation suites consist primarily of Microsoft Office.

Attachments referenced in Section J depict the current configuration and status of networks covered under the TO's current footprint.

C.2.3.1. NIPRNET (ULAN/UWAN)

The EUCOM/AFRICOM ULAN has wide-area connectivity to the Non-secure Internet Protocol Router Network (NIPRNet) and extends to remote sites including the Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium, to the HQ EUCOM Liaison Office (ELO) in the Pentagon, Washington, DC and to Camp Lemonnier, Djibouti.

The United States Army, Europe (USAREUR) is the Executive Agent for EUCOM/AFRICOM, and provides the NIPRNet infrastructure to include connectivity over the recently installed Installation, Information and Integration Modernization Program (I3MP). The ULAN is connected to the Army's NIPRNet gateway. The Army provides the NIPRNet circuit for the ULAN.

Note: ULAN/UWAN and NIPRNet terms are used interchangeably. However, the ULAN terminology specifically refers to the EUCOM portion of the unclassified network and is used to distinguish between the local portion of NIPRNet infrastructure used by EUCOM and the external NIPRNet connectivity provided through USAREUR.

C.2.3.2. SIPRNET (SLAN/SWAN)

The EUCOM/AFRICOM SLAN has wide-area connectivity to the Secure Internet Protocol Router Network (SIPRNet) and extends to remote sites including the Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium, to the HQ EUCOM Liaison Office (ELO) in the Pentagon, Washington, DC, and to Camp Lemonnier, Djibouti.

Defense Information Systems Agency (DISA) directly provides the SIPRNet service for the SLAN. SLAN network is propagated through a secure distribution system and runs out to distribution points in the buildings. It then routes to each end user at EUCOM/AFRICOM. Any workspace that does not have access to the distribution points uses Inline Encryption Devices (INE) over their unclassified circuits.

The EUCOM/AFRICOM Networks SLAN will use the Gigabit or greater connectivity to the fullest extent possible. At a minimum, physically redundant capability will be provided while funding and fielding are pursued to provide the required diverse routing. Multi Protocol Label Switching (MPLS) VPN COI architecture can be used over the GIG when the capability is available to provide the EUCOM/AFRICOM Network logical separation from the NIPRNet/SIPRNet.

Note: SLAN/SWAN and SIPRNet terms are used interchangeably. However, SLAN terminology specifically refers to the EUCOM portion of the secure network and is used to distinguish between the local portion of SIPRNet infrastructure used by EUCOM and the external SIPRNet connectivity provided by DISA.

C.2.3.3. COALITION/MULTI-DOMAIN NETWORKS

EUCOM/AFRICOM have responsibility for the operations and maintenance of C4 coalition systems. Joint war-fighting operations demand responsive information exchange across combined forces and unified commands for planning, unity of effort, decision superiority, and decisive global operations. Coalition systems and networks are a combination of global, regional, local, multilateral and bilateral, virtually separate networks supporting multinational efforts. Coalition and bi-lateral local area networks/wide area networks (LAN/WAN) include, but are not necessarily limited to, Combined Enterprise Regional Information Exchange System (CENTRIXS).

EUCOM/AFRICOM is responsible for the operation of existing coalition network systems as well as the integration, migration, and acceptance of new systems and capabilities into the existing architecture. EUCOM/AFRICOM has responsibility for all aspects of support surrounding these networks and systems: system administration, security, certification and accreditation user account management, hardware maintenance, configuration management, software licensing, training, and other forms of user support.

In the future, the coalition network responsibilities under this Task Order could extend to Molesworth and the requirements for the number of nodes/locations supported could grow or change, dependent on mission needs of the Government and partner nations. At present, there is a potential for 14 additional sites; however the expansion of coalition networks to other locations, including other sites within the AFRICOM AOR could be identified for inclusion during performance. Such work could entail: performance of site surveys to support deployment of coalition networks; supporting AFRICOM coalition CND/IA requirements; providing coalition network end user support; coalition network support; service desk and general operations and maintenance support. The Contractor would be expected to scale support up or down during performance as mission needs demand.

C.2.3.4. FUTURE CONSIDERATIONS

While the Local Area and Wide Area networks must be accredited to connect to the Defense Information Systems Network (DISN), future considerations should include the following:

- The EUCOM/AFRICOM Networks will implement the Department of Defense's (DoD) net-centric enterprise services and data strategy where possible to further their goals in trying to reach a true joint net-centric enterprise solution.
- The EUCOM/AFRICOM next generation enterprise networks will support net-centric operations for the larger Joint Network Environment.

- The EUCOM/AFRICOM Networks will be a key enabler for the war fighter and business operations of the combatant commands and will provide net-centric capability that improves the enterprise IT services currently provided.

Key initiatives include the COCOMs movement to the Joint Information Environment (JIE). The JIE Increment 1 is a regional initiative between 5SC, Network Enterprise Technology Command (NETCOM), Defense Information Systems Agency (DISA), AFRICOM, and EUCOM to consolidate IT infrastructures within the European Theater. JIE is a Department of Defense (DOD) level effort designed to collapse and consolidate the way IT services are provided across the DOD. The initiative looks at improving DOD's cyber posture through standardizing information assurance configurations; consolidating Service Component IT infrastructures into a common joint capability; streamlining network operations under a single joint construct; and providing a common IT governance structure for all of DOD.

As part of the initiative, AFRICOM has already transferred much of it's IT service responsibility to 5SC who in turn are using an existing Government workforce and in-sourcing current contracted positions, as well as well as leveraging this and other contracts to accomplish the mission. As a result the Contractor must be able to adapt and work in a mixed IT environment consisting of Active Duty, Government civilians, and other contractor personnel.

JIE has already had some successes too. We have already seen progression with the migration to Enterprise E-mail on the NIPRNet and the expected migration on the SIPRNet. Near future service areas to migrate could include Storage and Portal.

In pursuit of DoD's desire for standardization, IT service consolidation, efficiencies and economies of scale, future changes may include providing support under the scope of this Task Order to other DoD organizations in the context of JIE. It is envisioned that surge and optional CLINs may be utilized to address such future organizational requirements via Task Order modifications.

Additionally, EUCOM has initiatives underway and anticipates needing contractor assistance in developing and implementing a Data Center Consolidation Implementation Plan to assist in meeting DoD planned efficiencies that call for:

- Reducing total number Operating Systems (OS) by >30%
- Increasing OSs per Full-time Equivalents to >40
- Increase virtualization to >80%
- Increasing virtual OSs per host to >8

The plan will need to demonstrate how EUCOM supports the DoD's minimum data center target of 60% by FY18.

C.2.3.5 Commercial Solution for Classified (CSfC) Grey Network

EUCOM has implemented a Commercial Solution for Classified network named FLAGSHIP in accordance with and approved for use by NSA. FLAGSHIP is a “grey” network which utilizes a layered architecture of Commercial Off The Shelf (COTS) equipment and public domain algorithms which satisfies the Information Assurance controls that are mandated for providing transport of classified networks. CSfC uses Capability Packages (CP) which contain product-neutral information that allows customers to build their solution based upon their specific needs. FLAGSHIP has implemented the Virtual Private Network (VPN) CP and is awaiting approval of their Data At Rest (DAR) CP for approval, in addition the Mobility CP is being engineered for approval.

Currently FLAGSHIP is expected to provide limited transport services for access to the EUCOM SIPRNet domain only to approximately 100 endpoint devices. Endpoint devices may consist of laptops, tablets, or home kits (for use in VIP quarters). The customer base extends beyond EUCOM personnel to include US Military personnel in Europe (ie AFRICOM, NATO, SOCEUR, SOCAfrica, USAFE. USAREUR…etc).

FLAGSHIP is identified as a MAC-II system and provide the contract’s full range of services. VIP’s shall be as currently identified for EUCOM and as supplemented by EUCOM J65 for non-EUCOM personnel (mainly other General Officer and/or SES personnel).

Future Considerations: Expand FLAGSHIP to provide transport for additional EUCOM managed domains such as Centrixs, Seagull, and/or US BICES. Additionally, EUCOM is exploring the possibility of providing FLAGSHIP as a transport service for other non-EUCOM managed domains such as AFRICOM, SOCEUR, and USAREUR. Implementing either of these considerations would require expanding the Grey Network by providing enclave level services such as Active Directory, HBSS, automated scanning…etc. therefore added services would also need to be considered.

C.3. SCOPE

The scope of this Task Order covers the requisite labor to perform the technical, program management, administrative, documentation and reporting services detailed in Section C; the logistical support defined in the annexes; the Other Direct Costs, Travel, and Tools necessary and ancillary to performance; and the potential for Optional Services to be invoked as a unilateral right of the Government.

C.4. OBJECTIVES

The objectives of this Task Order are to provide communications and IT services and procure state-of-the-industry communications and information technology assets. The Government seeks an Industry partner that can:

- Provide flexible, scalable IT services that will enhance each supported activity’s ability to respond to dynamic needs in their respective areas of responsibility.
- Deliver operational, technical and program efficiencies to drive down costs without compromising the timeliness or quality of services.
- Optimize use of tools, technologies, bandwidth, capacity, and computing power in a manner that controls and reduces costs.
- Provide a best-of-breed approach and meld industry best practices with each supported activity functional expertise to develop optimal solutions to current and future command challenges.

- Manage workload surges effectively and in a manner that, given mission requirements and competing priorities, efficiently schedules and applies resources to meet the needs of supported activities without one activity's needs being given primacy over the other.

C.5. REQUIRED TASKS

C.5.1. GENERAL

C.5.1.1. STAFF

The Contractor shall provide the requisite number of technically qualified personnel with appropriate security clearances and information assurance (IA) certifications to perform the communications and information technology operations and maintenance (O&M) and European-African theater communications and IT planning tasks as specified under this PWS.

Note: See Section H for security clearance and IA certification requirements.

C.5.1.2. REGULATIONS, DIRECTIVES, AND STANDARDS

The Contractor shall follow Government regulations, directives, and standards while applying industry best practices and standards to the maximum extent possible. Contractor personnel shall have an understanding of these best practices, regulations, directives, and standards as appropriate for their specialized areas. The Contractor shall perform the work on this Task Order in accordance with (i.a.w.) the guidance listed in Attachment A – Specific Governing Documents and i.a.w. other documentation referenced elsewhere in this Task Order. This guidance is updated periodically over the period of performance and the Contractor shall perform the work on this Task Order i.a.w. the latest updates.

C.5.1.3. DELIVERABLES

Deliverables are indentified throughout Section C and a consolidated list is included in a Deliverables Schedule in PWS section C.5.13.7. The format of specific deliverables shall be proposed by the Contractor and agreed to by the Government.

C.5.1.4. HOURS OF PERFORMANCE (*Note: See Section F for additional requirements)*

C.5.1.4.1. 365 / 24 / 7 ON-SITE PRESENCE

The Contractor shall provide a 365/24/7 on-site presence in Stuttgart, Germany (either on Patch Barracks or Kelley Barracks) and on Camp Lemonnier, Djibouti. The Contractor's designated point(s) of contact must be able to triage the reported outage and contact on-call personnel when required. It is expected that the on-site POC will be able to perform normal duties as assigned.

The Contractor shall proactively monitor networks/systems that are within their purview using the Government provided toolsets (e.g. 5SC managed Remedy-based NetOps Support System (NSS), Net monitoring tools, EUCOM Service Desk, etc.).

C.5.1.4.2. ON-CALL SUPPORT

The Contractor shall provide on-call support for exceptional or emergency requirements which occur outside of normal duty hours. Exceptional or emergency requirements are defined as:

- All Maintenance Priority 1 and 2 outages to include VIP end user devices

- All Maintenance Priority 3 outages involving systems, network equipment, and VTC suites but not to include non-VIP individual end user outages.

Note: See PWS section C.5.1.5.2 for Maintenance Priorities definitions

The Contractor shall establish procedures (to include on-call rosters) for each COCOM and CLDJ to be approved by each TPOC. The Contractor shall respond telephonically to an outage with a technician qualified in the required service area within:

- 1 hour of notification for all locations except HOA.
- 30-minutes of notification for HOA.

The Contractor shall respond on-site with a technician qualified in the required service area within:

- 2 hours of initial notification should the outage remain unresolved - for all locations except HOA.
- 1 hour of initial notification should the outage remain unresolved - for HOA.

On-site troubleshooting shall continue for as long as the outage remains unresolved.

Note: On-duty personnel may provide initial response however should the outage/problem remain unresolved they shall notify the on-call designated subject matter technician within the aforementioned time periods.

C.5.1.4.3. OPERATIONS AND EXERCISE SUPPORT

The Contractor shall participate in all operations and exercises, consistent with the level of service specified by the Government's technical direction. The scope of operations and exercise support includes, but is not limited to:

- Configuring and deploying hardware to support the operation/exercise
- Establishing new or expanding existing network services
- Establishing new or expanding existing Operation Centers
- Troubleshooting and resolving network and user problems

Requirements for providing operations/exercise support do not include providing support for Tactical Communications or Systems. Contractor support is limited to extending existing network services to the applicable remote sites as described in PWS sections C.2.2.2 and C.5.4.4. Travel may be required and while these sites may be austere, the Contractor shall not be required to deploy (travel) under field conditions.

Note: Requirements described in this section are applicable to networks, services, and systems supported and described in the various attachments. Other Operation/Exercise support may be deemed in scope but may be accomplished by exercising a unilateral optional requirement from PWS section C.6.

The Contractor shall not increase manpower or man-hours for Operations or Exercise participation unless authorized by the Contracting Officer (CO) or the Contracting Officer's Representative (COR).

C.5.1.4.4. OPERATIONS SUPPORT

Operations are typically unannounced and have an unknown duration. The Contractor may be required to surge current work force to meet 24x7 operation needs. As much as possible this surge should be satisfied within existing staffing levels and without degradation of service. However, if needed the

Contractor may request overtime and/or relief from service levels from the Government. Should operations continue long enough the Government may require or the Contractor may request additional resource be brought in TDY to meet mission needs.

C.5.1.4.5. EXERCISE SUPPORT

Exercises are planned events therefore although additional work may be required there should be sufficient time to schedule the work to not impact current operations. Normally exercise scenarios progress on a non-mission interference basis during normal duty hours. The Contractor shall coordinate with the Government to adjust staff schedules to support exercises while concurrently delivering ongoing day-to-day services and support within the available staffing levels. Where directed by the Government, the Contractor shall provide 24x7 coverage during the exercises. This may include adjusting the normal work schedule or minimizing/prohibiting leave of individual contractor employees to achieve the required coverage.

C.5.1.5. MAINTENANCE

The Contractor shall provide and perform maintenance for all AFRICOM/EUCOM/CJTF-HOA *contractor supported equipment* communications and IT network systems, and devices, to include, but not limited to, the ULAN, SLAN, coalition, command and control, and other supported networks and systems, inclusive of:

- Windows-based, Oracle Solaris UNIX-based servers, and LINUX-based servers such as ACAS;
- Windows-based, Oracle Solaris UNIX-based, and MAC-based workstations, laptops, or tablets
- Thin clients/zero client terminals;
- Printers and scanners connected to the AFRICOM/EUCOM/JTF-HOA networks;
- Video teleconferencing equipment;
- LAN hardware including hubs, routers, and switches;
- Connectivity devices from network drops to desktop; and
- End-user network-related telephony devices.

Refer to Section J attachments for additional network, architecture, hardware/software and warranty information.

The Contractor shall ensure all supported hardware is repaired under warranty prior to issuing separate orders for repair, when possible. Should it become uneconomical to repair a piece of equipment, the TPOC will determine whether or not to fund the repair or the replacement of an item. The Contractor shall maintain spare and repair parts inventory and property accountability.

The Contractor shall develop and implement a standardized maintenance program for all contractor supported equipment as shown in the Supported Equipment List based on DoD guidance, industry standards or best practices, Original Equipment Manufacturer (OEM) service manuals, Service-based Technical Orders (TO) and established local procedures. The program shall include recurring preventive maintenance, and non-recurring priority 1 – 4 maintenance to include: installation, removal, modification, troubleshooting, fault isolation, repair, replacement, reprogramming, or reconfiguration of equipment, systems, or networks. The program shall not include replacement or provisioning of consumables (e.g. paper, ink, or toner for printers).

C.5.1.5.1. MISSION ASSURANCE CATEGORY (MAC)

The Contractor shall ensure applicable networks are configured, maintained and documented i.a.w. the assigned MAC level and Confidentiality Level (CL). The following MAC information (excerpted from DoD Directive 8500.01E, "Information Assurance (IA),") is applicable:

The MAC reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. MACs are primarily used to determine the requirements for availability and integrity. DoD has three defined mission assurance categories:

- <u>MAC I</u>: Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.

- <u>MAC II</u>: Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure adequate assurance.

- <u>MAC III</u>: Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

C.5.1.5.2. MAINTENANCE PRIORITIES

<u>Maintenance Priority 1 – CRITICAL</u> – is assigned to:

- Outages of all MAC I systems and equipment
- Outages of systems and equipment supporting each COCOMs Top 5 VIPs to include office, home, and mobile locations
- Outages deemed critical by personnel authorized to give technical direction to the contractor under this contract

<u>Maintenance Priority 2 – URGENT</u> – is assigned to:

- Outages of MAC II systems and equipment affecting more than 25% of users
- Outages of MAC II systems and network equipment supporting local/national emergencies
- Outages of equipment and systems supporting all other VIPs not defined in Priority 1 to include office, home, and mobile locations
- Outages deemed serious by personnel authorized to give technical direction to the contractor under this contract

<u>Maintenance Priority 3 – HIGH</u> – is assigned to:

- Outages of MAC II systems and network equipment affecting less than 25% of users
- Outages of MAC III equipment and systems more than 10% of users
- Outages of bridge-type (conference room) VTC suites
- Individual end user outages rendering assigned desktop/laptop workstation inoperative
- Outages deemed a priority by personnel authorized to give technical direction to the contractor under this contract

Maintenance Priority 4 – ROUTINE – is assigned to:

- Outages of MAC III systems and network equipment affecting less than 10% of users
- All end user outages not otherwise defined
- All scheduled maintenance that do not meet the definitions of Maintenance Priorities 1 – 3

C.5.1.5.3. ADDITIONAL SPECIFIC TASKS

The Contractor shall:

- Develop and maintain a standardized Maintenance Management Plan. The Maintenance Management Plan shall include all processes and procedures used to implement the Contractor's standardized maintenance program.
- Incorporate available maintenance agreements and warranty contracts for parts and labor on supported equipment into their maintenance program.
- Schedule and perform maintenance that affects user services after core hours of operation, whenever possible, in order to minimize user impact.
- Coordinate and schedule outage requests for equipment maintenance i.a.w. 5SC, AFRICOM, EUCOM, and/or CJTF-HOA procedures governing this process.
- Notify the government before starting and upon completion of all Priority 1 or 2 maintenanace actions on operational equipment.
- Provide an estimated repair time to the designated Government representative within 1 hour after initial response for all Priority 1 & 2 maintenance actions.
- Provide updated status for all Priority 1 & 2 maintenance actions at intervals requested by the reporting activity, when it is known the estimated repair time will be exceeded, or upon repair/restoral, whichever is sooner.
- Document all maintenance actions into the government designated maintenance management system.
- Provide the Government a summary report of all maintenance actions to include preventive maintenance inspections and services.
- Provide Data Center/Communications Closet facility management support include:
  - Monitoring Heating, Ventilation and Air-conditioning systems and power and notifying the Service Desk, Watch Officer and TPOC of any issues,
  - Server and Network rack and cable management,
  - Monitoring the facilities for adverse environmental conditions.

C.5.2. COMMON REQUIRED TASKS

These enterprise level tasks are required by AFRICOM, EUCOM, and CJTF-HOA and may be provided as shared services, customer specific, or both (i.e. AFRICOM and EUCOM shared, CJTF-HOA stand-alone). The Contractor shall provide analysis, administration, maintenance, and technical support for hardware, software, procedures, and peripheral equipment for the various networks, enclaves and systems that make up the AFRICOM, EUCOM, and CJTF-HOA information systems. These information systems shall provide services to a range of joint service end points that include data, voice, and video users; a mix of end-user accounts, and interfaces to other COCOM and DoD communications environments.

C.5.2.1 SYSTEM ADMINISTRATION SERVICES

The Contractor shall provide continuous system administration services for AFRICOM, EUCOM, and CJTF-HOA information systems as shown in Attachment B entitled "USAFRICOM C4 Systems Overview" and Attachment C entitled "USEUCOM C4 Systems Overview". System Administration services consist of common system administration tasks, system security tasks, and system capacity planning tasks.

C.5.2.1.1 COMMON SYSTEM ADMINISTRATION TASKS

The Contractor shall perform the following common system administration tasks:

- Analyzing system logs and identifying potential issues with computer systems.
- Introducing and integrating new technologies into existing data center environments.
- Performing routine audits of systems and software.
- Performing backups and data recovery
- Applying operating system updates, patches, and configuration changes.
- Installing and configuring new hardware and software.
- Adding, removing, or updating user account information
- Answering technical queries and assisting users.
- Responsibility for documenting the configuration of the system.
- Troubleshooting any reported problems.
- System performance tuning.
- Configure, Add, Delete File Systems

C.5.2.1.2 SYSTEM SECURITY TASKS

The Contractor shall perform the following system security tasks:

- Maintain all system devices (servers) i.a.w. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS) and CYBERCOM taskings
- Take appropriate measures to respond to known and possible network attacks i.a.w. applicable DoD policies, directives and instructions, or as directed by the CND Service provider.
- Ensure all Contractor managed items are configured to store and archive all system, device, application, and security event logs i.a.w. DOD and (if applicable) NATO security policies.
- Auditing and reviewing all system, device, application, and security event logs i.a.w. DOD and (if applicable) NATO security policy
- Reporting, mitigating and/or resolving all classified security incidents (e.g. data spills) that impact AFRICOM networks within time constraints identified by the applicable directive or as directed by the Computer Network Defense (CND) Service Provider
- Supporting incident reporting activities i.a.w. CND Service Provider and AFRICOM policies
- Supporting and providing the necessary information (i.e. firewall logs, system logs, storage media, etc.) to the Stuttgart Regional Network Analysis Lab (SR NAL) and other government designated organizations in the performance of forensic analysis services

C.5.2.1.3 SYSTEM STORAGE CAPACITY PLANNING

The Contractor shall assist the Government in identifying and matching the storage needs of Contractor operated and maintained systems to allocated storage space. The Contractor shall perform assessments as to whether there are potential problems and issues that must be addressed, and provide the results to the Government. The Contractor shall provide the following storage capacity related services:

- Follow the Backup and Recovery plans to ensure there is no application performance degradation according to service-level agreements
- Manage allocated storage to avoid incidents caused by lack of capacity
- Justify and request additional storage should it become necessary

C.5.2.2 CONTINUITY OF OPERATIONS (COO)

The Contractor shall provide for the operation and support of the Government designated COOP sites in the event current services/facilities are inoperable and will remain so for an undetermined amount of time. Enclave boundary defense and security measures at the COOP site equivalent to must be equivalent to the primary site. The Contractor shall provide analyses, engineering assessments, preliminary studies, and recommendations to assist in the IT portion of the current COOP plan as well as establishing and fielding their next-generation COOP capability.

C.5.2.2.1 COOP INFRASTRUCTURE/CAPABILITIES

The Contractor shall perform the following COOP tasks:

- Maintain an alternate command and control capability per the Government plan.
- Manage transition of mission essential operations within specified time frame.
- COOP site maintenance and testing, as directed.

C.5.2.2.2 COO PLAN

The Government's requirement is to exercise and report DRP and COOP on at least an annual basis. The Contractor shall participate in COOP exercises on a regular basis as directed by the Government to ensure complete functionality as defined by the plans. The Contractor shall develop and provide the Government with a specific COOP exercise plan based upon stated Government requirements and objectives for each exercise at least 30 calendar days prior to the anticipated start date of the exercise. Post exercise the Contractor shall provide an assessment of the exercise.

The Government's requirement is to maintain a hard copy of the DRP and COOP at the primary and alternate site. Alternate site maintenance shall be as specified by the Government.

C.5.2.3 REMOTE EXTENSION - WASHINGTON LIAISON OFFICES

The Contractor shall provide Systems Analysis, System Engineering, and System Administration services to AFRICOM and EUCOM Washington Liaison Offices (LNO) in the Pentagon, Washington, DC. The Government will require permanent support at this location to provide systems administration support, as well as temporary travel to this site on occasion for server upgrade and firewall support. The Contractor shall provide the following services:

- Configure and administer end-user workstations, servers, and network devices i.a.w. established standards
- Provide an operational connections to AFRICOM and EUCOM support enterprise networks and provide local services (to include email, shared file storage, network printing, domain name service, internet protocol address management, and Defense Message System)
- Provide audiovisual/VTC support (such as Tandberg desktop VTC)
- Provide hardware maintenance on installed workstations, printers, firewalls, routers, switches, servers, and network equipment
- Ensure configuration management procedures enforce accreditation policy requirements to maintain network accreditation
- Provide informal over-the-shoulder user training as required

- Provide network planning support and analysis for any relocations or office consolidations of the LNO

C.5.2.4 PORTAL TECHNOLOGIES

The Contractor shall provide communications and IT O&M support for hardware and software identified by the Government as necessary for portal capabilities. Currently AFRICOM, EUCOM, and CJTF-HOA have separate contracts to provide application development hence the references to the "Application Development Team". The Contractor shall perform specific duties that include but are not limited to:

- Install, configure, and troubleshoot the production system and associated applications in all environments
- Perform system administration, domain administration, network administration and Lab engineering & administration
- Support OS/Virtualization and other unique services which include ADFS, Integration, REL, and Identity Management
- Maintain system administration and day-to-day operations on the development network
- Install, integrate, test, and deploy applications i.a.w. approved test plans
- Partner with application development team to help solve business needs
- Administer and support infrastructure technologies in the Collaboration and Content Management space to include but not limited to: CRM, BI, OCS/LYNC, MOSS, SharePoint
- Upgrade the various technologies as required
- Complete assigned day-to-day support ticket requests for the above technologies

C.5.2.4.1 COLLABORATION SERVICES

The Contractor shall provide Systems Analysis, Systems Engineering, System Administration, Information Assurance, and end-user support services for the Collaborative Information Environment (CIE) which includes primarily web-based tools required for collaboration, planning, and operational support. The Contractor shall perform specific duties that include but are not limited to:

- Oversee the SharePoint application portfolio on SIPR and NIPR networks
- Integrates / configures .NET applications and SharePoint technologies with SQL Server database
- Maintain the various SQL databases supporting OCS/LYNC, CRM/TMT, and IIS/Web Applications
- Monitors performance of SharePoint architecture and web based applications after implementation
- Serves as the central point of contact for SharePoint activities and acts as a liaison for users, content owners, team site administrators and the Application Development team
- Advises the Content Librarian or Content Manager, and the Content Coordinator(s) on proper document profiling and customization for Corporation Portal (SharePoint);
- Performs SharePoint administration to configure settings that affect the system service, such as load balancing for indexes; to setting priorities for applications;
- Performs stress testing and other operations on the web storage system, the dashboard site, SharePoint servers and web parts, to assure optimal system performance
- Maintains application documentation to describe software components development, logic, coding, testing, changes, and corrections
- Assists the Application Development Team in the full lifecycle development of portal applications/parts including functional requirements, analysis, and user interface design, database design, security control setup, testing and documentation
- Operate and maintain desktop tools to provide end users with the ability to fully utilize the collaboration functionality such as OCS/LYNC.

C.5.2.4.2 WEB SERVICES

The Contractor shall provide Web design and administration services to AFRICOM and EUCOM Web-based systems for the each respective Public Affairs Office. The scope of services includes planning, designing, testing, and implementing static and dynamic Web pages, Web sites, Web applications and associated content. The Contractor shall deliver production management, Web page design, markup languages, scripting, and relevant Web services support. Web services changes to the communications and IT baseline shall be planned and implemented i.a.w. established, formal configuration management and change control processes. The Contractor shall apply knowledge, skills, and strong user interface design experience, along with Web development experience to:

- Ensure web content provided is optimized in a manner that motivates, entertains, educates, engages, and appeals to the user community such that it encourages regular access and use as a major source for information and decision making.
- Produce site-maps, wire-frames, mock-ups (without graphics design), and style-guides.
- Design, develop, and maintain a consistent information architecture, user interface features, site animation, and special-effects elements to ensure predictable, successful user interactions.
- Create scripts/code that interacts with Web servers, the content for Web-based systems, and provides dynamic Web content through the Web/internet servers.
- Seek user community feedback and input for improving and enhancing Web sites.
- Develop and implement standards/guidelines subject to Government approval.
- Advise and coordinate with content developers on requirements, and applicable standards.
- Contribute to the design group's efforts to enhance the look and feel of the online offerings.
- Research and recommend Web-technologies with respect to the distribution of content, collaboration, and information sharing.
- Identify and resolve technical issues with Web-based systems and content.
- Apply appropriate security measures; provide for the appropriate use of copyrighted material; and produce reports and other documentation.

C.5.3 AFRICOM REQUIREMENTS

The Contractor shall provide **dedicated resources** to deliver these requirements. A dedicated resource means AFRICOM will fund the full cost of the employee to include staffing-related Other Direct Costs therefore expects all of the resource’s basic labor hours to be spent on AFRICOM work.

C.5.3.1 CUSTOMER SUPPORT SERVICES

The Contractor shall provide technical support to end users to include:

- Managing of user accounts and SIPR/Alternate Tokens
- Providing dedicated end user service technicians when specified by the Government
- Respond to user telephonic and electronic requests for assistance
- Extended service hours to support real world operations and exercises

C.5.3.1.1 ACCOUNTS MANAGEMENT

The Contractor shall provide a consolidated account management service desk which provisions and de-provisions IT systems accounts as personnel are assigned to or departing from AFRICOM. The Account Service Desk shall be open during normal business hours (M-F, 0800-1700) except for US Holidays. Assigned contractor staffs are required to certify and perform as Enhanced Trusted Agents (ETAs) for SIPR/Alt Token services. Account management services shall include as a minimum:

- Validation of 8570.01 requirements

- Account creation/deletion
- Updating of GAL information
- Issuance and management of User Agreements
- PKI Token services (issuance, reconstitution, PIN resets, revocations, out-processing)

C.5.3.1.2 PKI TOKEN SERVICES

The Contractor shall provide Enhanced Trusted Agent (ETA) services as the SOLE provider for AFRICOM during normal work hours. It is expected that the majority service required will be on a walk in basis. These services shall be provided from the Consolidate Account Management Service Desk for AFRICOM. Token services shall include as a minimum:

- Train and certify all Accounts Service Desk personnel to perform as ETAs
- Troubleshooting and resolving Token Card failures to include PIN resets
- Requesting certificates for new or reconstituted cards from the Local Registration Authority
- Printing and issuance of tokens/cards
- Revoking tokens when required

C.5.3.1.3 CUSTOMER IT SUPPORT SERVICES

The Contractor shall provide AFRICOM desk-side touch and application support services for IT end user device issues to assigned building and/or customer base. The Contractor shall provide immediate desk-side service to mission critical users for IT related issues which may include:

- Problem recognition, research, isolation, resolution, tracking, and follow-up
- Tier 2 support to end users for desktop, thin client, network, applications, or hardware
- Coordinate and interact with IT service provider
- Recommending hardware. software, and modifications to meet end user requirements and/or mitigate issues
- General touch labor support

This requirement may require the Contractor to provide support during Command Operations that will require work hours falling outside of normal duty hours therefore alternate work schedules. Normal duty hours are defined as Monday through Friday 0700-1800. Contractor employees shall be dedicated to assigned building and consider the building as their prime work locations. Customer IT Support Specialist services are required for the following locations:

- Bldg 3304 SOCAF
- Bldg 3314 Command Section
- Bldg 3315 J2/J3
- Bldg 3322 JOC
- Bldg 3350 J3

Changes to building locations may be specified during performance.

C.5.3.1.3.1 AFRICOM JOC CUSTOMER IT SUPPORT SERVICES

AFRICOM has built a new Joint Operations Center in building 3317 and requires increased operations support. The AFRICOM JOC consists of several key areas including the Senior Decision Cell, the Watch floor, three Operation Center Rooms, three Action Cells, Conference Rooms, Team Rooms, Theater Rooms and Telecommunication Rooms. The current JOC CSA supporting bldg. 3322 shall transition to support the new JOC as the facility becomes functional and be supplemented with two additional CSAs.

Normal duty hours for JOC support are increased to Monday through Friday 0700-2200. When services are required outside of normal duty hours due to mission needs, the Government should provide at least 24-hour notice.

Fully supported services are SIPR and NIPR Computers (desktop, latop, VDI clients, and/or tablets) , printers, and other peripherals (includes the Active DCO computers).

Partially supported (defined as device connectivity and user maintenance) services for: Coalition network (BICES, CENTRIX, SEAGULL) computers and devices; Coalition, NIPR, and SIPR Audio-Visual Desktop devices (Tandbergs, etc.); VOIP devices (Coa;ition, NIPR, VOSIP, ECVOIP); IPTV, and Smart Boards.

[Note: Reference PWS Attachment B.11 AFRICOM JOC Conceptual Drawing for details.]

Other:

- The Facility has been declared a Special Security Area therefore Contractor employees will require a Top Secret clearance with SCI access Security Clearance

C.5.3.1.4 COALITION NETWORK END USER SUPPORT

The Contractor shall provide end user support for various Coalition systems i.a.w. the requirements for communications and IT support as described in this document. The desktop baseline consists of a workstation, VOIP, and associated peripherals. Networks to be supported include SEAGULL with approximately 10 desktops and a VTC Suite and CENTRIXS GCTF and CENTRIXS CMFC both with approximately 5 desktops. The end users/desktops are located on the Kelley campus with about half in the facilities named in the previous paragraph. The requirements for these coalition systems can be expected to grow over the next year, in some cases maybe doubling.

The Contract shall also provide network engineering support as required to initiate and maintain these coalition services in the requested facilities.

Reference PWS Attachment C – U.S. BICES Architecture Diagram

Coalition/Partner Networks are:

- Defined as any network that is utilized by USAFRICOM/CJTF-HOA for mission purposes that contains non-DoD endpoints. Typically connectivity is provided via a tunnel through AFRICOM's existing network.

The Government is seeking a tiered support structure (such as that outlined below) tailored to provide responsive services within each tier to enable effective support to the mission. The scope encompasses base line support covered under this Task Order.

- I: Touch labor to ensure transport to include tunnel is active and end point has IP services. (e.g., CMFC)
- II: Tier I plus management of some localized services/servers and desktop support (imaging and touch labor) (e.g., GCTF)
- III: Full network that is engineered, designed, O&M'd by USAFRICOM/CJTF-HOA (e.g., ADSN)

A simplified construct that is flexible and can be utilized to service any network AFRICOM utilizes is desired.

C.5.3.2 VIRTUAL DESKTOP INFRASTRUCTURE (VDI) O&M SERVICES

The Contractor shall provide Operations and Maintenance support to include applicable IA services for AFRICOM's VDI infrastructure for desktop presentation in single or multi-level security environments. The Contractor shall be responsible for O&M on all servers, storage, applications, and network equipment as identified in Attachment C - AFRICOM VDI Diagram. O&M services encompass support for the current Phase 1 VDI server environment, VDI Storage Area Network, CITRIX desktop environment as well as user end points connected to the applicable network. These services span other PWS requirements (i.e. system administration, network management, configuration management, information assurance, storage management, etc…) described elsewhere in PWS section C.5 - REQUIRED TASKS.

C.5.3.3 COMMAND AND CONTROL (C2) SYSTEMS, APPLICATIONS, AND SERVICES

The Contractor shall provide C2 systems applications and services support for AFRICOM in the areas of systems engineering; server configuration; software engineering; and display management. This support is limited to what is allowable by Global Command and Control System - Joint (GCCS-J) Program Management Office (PMO). In addition, this PWS is intended to provide O&M services as it relates to IT and not Operator Services (such as Common Operating Picture management).

AFRICOM has 1 instance of GCCS-J requiring support and SOCAFRICA has 1 instance of GCCS J- requiring similar support. It should be noted that the support for the SOCAFRICA instance will be priced separately under the SOCAF subCLIN. The Contractor shall provide the following C2 system support:

- Procurement of hardware with minimum specifications as determined by the PMO and GOTS developer.
- Proposed device connectivity as determined by the PMO and GOTS developer.
- Proposed rack space design for servers with proper cooling systems.
- Installation of GOTS and Government-provided equipment and software that is not proprietary and does not require specialized installation.
- System Administration; System Maintenance; Technical Refresh/Upgrade Support.

C.5.3.4 SYSTEM ENGINEERING SUPPORT

The Contractor shall provide Network and System Engineering Support services to improve customer service, system performance, and reliability for the C4 Networks and Systems for projects as designated by AFRICOM.

The Contractor shall provide Network and System Engineering Support services to improve customer service, system performance, and reliability for the C4 Networks and Systems for projects as designated by AFRICOM. AFRICOM requires a holistic approach to engineering beginning with the planning process. The Contractor shall apply DoD Unified Capabilities objectives and tenets to engineer AFRICOM's solution to support efforts to share and distribute information by electronic means. The Contractor shall look beyond the technological requirements to examine the business processes that are driving those needs. The Contractor's engineering approach allow for testing prior to delivery, internal quality checks during the engineering phase as well as Quality Assurance during the migration and transition phase, and disaster recovery requirements built into the solutions. Finally, service migration is more than new technology or platforms; it is moving the users to the new service and addressing/overcoming their needs and fears.

The Contractor's engineering processes will span other areas of this PWS. Logistical support areas such as tool purchasing, asset management, and configuration management will be integral to many of the engineering projects. Information Assurance service area of Architecture and Engineering will assure that required security controls are addressed in the solution.

The Contractor may or may not have full control of the Engineering projects they are assigned. Depending upon the scope, size, complexity, and Government needs, the Contractor will often be a member of an integrated teams consisting of both Government and other Contractors. Project plans shall clearly identify the Contractor's roles and responsibilities.

The Government anticipates the need of the following disciplines in performance of engineering tasks:

Application Integration
Audio Visual Engineering
Data Architecture Engineering
Data Base Design and Architecture
Network Engineering
Project Management
Server Infrastructure Engineering
Storage Infrastructure Engineering
System Engineering
Technical writing
Unified Communication Engineering

Note: The disciplines anticipated may not be all inclusive. Additionally, inclusion of a discipline does not indicate that one FTE (a full man-year) is needed in that area nor on the other hand that one FTE will suffice.

C.5.3.4.1 CAPABILITIES PLANNING AND REQUIREMENTS ANALYSIS

The Contractor shall assist the Government by providing forward-thinking technical direction and engineering services for assessing system performance and business needs, planning for new and evolving C4 systems, evaluating proposals for the migration of existing services, and making recommendations for corrections and enhancements to current systems. Contractor planning services shall include providing draft documentation and technical input to documentation for assessments, plans, system implementations and architectures, and engineering designs related to new, evolving, and existing C4 systems. At the direction of the Government, the Contractor shall conduct and/or participate in strategic planning, studies, and evaluations to provide resource requirements, present recommended solutions, determine labor and tools estimates, and plan/refine schedules. The Contractor's effort shall include:

- Providing technical studies, reviewing plans, evaluating state of the technologies prior to fielding of new releases or systems
- Reviewing C4 plans and policies and providing observations and questions for consolidated responses
- Researching and coordinating technical issues and requirements and drafting new and updated policy governing technical issues
- Providing technical analyses and draft reports of C4 system tests, assessments, and architectures
- Participation in meetings as required by the Government to include attending conferences; technical interchange seminars; interoperability meetings; and other briefings related to integration, migration, and maintenance of C2, coalition, and bi-lateral system architectures

- Perform analysis, provide recommendations, and prepare planning documentation as directed by the Government for approval to transition current services into the JIE
- Planning large-scale systems and projects through vendor comparison and cost studies and provide input to policy level discussions regarding standards and budget constraints
- Developing Project Charter, Scope Document, and Requirements document as need to satisfy project needs
- Determining Life Cycle Replacement (LCR) needs of supported technology based upon industry standards and budget constraints. Develop and submit a semi-annual LCR plan for Government approval

C.5.3.4.2 ENGINEERING AND INTEGRATION

Based upon the outcome of Capability Planning and the Requirements Analysis, the Contractor shall provide emerging communications and information technology engineering support and technical solutions to improve overall service delivery to include customer support, network and system support, IT services, unified communications, storage…etc. The Contractor shall be required to design and build solutions for a wide range of IT projects ranging from the single product level to complex, large-scale, and/or enterprise-type projects. In addition as services and technologies evolve, new software and hardware will need to be incorporated into the existing baseline as determined by the applicable Government agent. Finally new security measures will be developed, issued, and require implementation therefore need to be integrated into existing baselines. To meet these requirements, the Contractor shall:

- Test and evaluate commercial-off-the-shelf applications, Government-off-the-shelf applications and hardware for integration into the C4 networks
- Ensure compatibility with current baseline, resolving conflicts as they arise
- Apply appropriate security measures (STIGs, IAVMs, Tasking Order Compliance…etc) to lock down the application/hardware
- Develop deployment procedures (i.e. package software, installation instructions…etc)
- Have Information Assurance review and sign-off acceptability prior to deployment
- Test and evaluate IA directed patches for compatibility with the current baseline and resolve any conflicts prior to deployment
- Provide design and engineering support for new network and system implementations and upgrades to include hardware, software, projection systems, video switching hardware, video teleconferencing, and other systems to meet project requirements
- Develop solutions to migrate services from the current environment to the COCOM approved JIE solution
- Provide Project Management using the Project Management Institute's (PMI) framework and following AFRICOM and 5SC processes
- At the Government's direction, develop and maintain the project plan to all sub-plans
- Ensure the engineering solution covers all phases of the project plan including removal of the old technology
- Determine training needs and recommend solutions for both the IT service provider and end user
- Engineer, install, operate and maintain a test lab in support of AFRICOM C4 networks.
- Provide effective technical solutions to complex problems to include Tier 3 troubleshooting of incidents or problems when requested

C.5.3.4.3 MIGRATION AND TRANSITION

The Contractor shall provide migration and/or transition support to implement approved engineered solutions into the ACIE. Migration and transition may range anywhere from moving a service to a new provider such as Enterprise E-mail, moving to a new or upgraded application or hardware, operating system upgrades, life cycle replacement…etc. The Contractor shall plan, document, and lead the transition of all system and network devices, including security devices, from the engineering team to the O&M team. The actual implementation team as well as the accepting O&M team may or may not be the Contractor's personnel. The Contractor shall:

- Draft documentation to include install instructions and configuration drawings and diagrams for the implementation and O&M team
- Provide over-the-should assistance when necessary to the implementation team
- Provide knowledge transfer on the new technology to the O&M team
- Perform Quality Assurance checks and/or Acceptance Testing as identified in the Project Plan and directed by the Government.
- Review as-built documentation for accuracy and potential problems

The Contractor may be required to use existing O&M personnel and/or surge personnel in order to implement the engineered solution

C.5.3.4.4 APPLICATIONS DEVELOPMENT SUPPORT

Note: AFRICOM engineering efforts include multiple cases of custom applications being written in C# or Powershell to enable the integration, management, or operation of software and systems in the Joint Information Environment (JIE).

The Contractor shall provide applications implementation and integration support to research, test, enhance, debug, implement, and integrate software on multiple platforms to include servers, desktops, and mobile devices for the Africa Command Information Environment (ACIE) and the Joint Information Environment (JIE).

The Contractor shall troubleshoot problems with software that is already in production to alleviate issues related to software applications (such as Forefront Identity Management, Active Directory, Systems Center Configuration Manger, TITUS, Task Management Tool, and others). Instructs, assigns, directs, and checks the work of other software developers on development team, where applicable.

The Contractor shall lead the development of software user manuals for production systems and systems developed by the contractor to support turnover to operations support teams.

C.5.3.4.5 REQUIREMENTS ANALYSIS SERVICES

The Contractor shall assist the Government in assessing system performance, planning for new and evolving C4 systems, evaluating proposals for the migration of existing functionality, and makemg recommendations for corrections and enhancements. Contractor planning services shall include providing draft documentation and technical input to documentation for assessments, plans, system implementations and architectures,and engineering designs related to new, evolving, and existing C4 systems. At the direction of the Government, the Contractor shall conduct and/or participate in strategic planning, studies, and evaluations to provide resource requirements, present recommended solutions, determine labor and tools estimates, and plan/refine schedules. The Contractor's effort shall include:

- Providing technical studies, reviewing plans, evaluating state of the technologies prior to fielding of new releases or systems
- Reviewing C4 plans and policies and providing observations and questions for consolidated responses
- Researching and coordinating technical issues and requirements and drafting new and updated policy governing technical issues
- Providing technical analyses and draft reports of C4 system tests, assessments, and architectures
- Participation in meetings as required by the Government to include attending conferences; technical interchange seminars; interoperability meetings; and other briefings related to integration, migration, and maintenance of C2, coalition, and bi-lateral system architectures
- Perform analysis, provide recommendations, and prepare planning documentation as directed by the Government for approval to transition current services into the JIE

C.5.3.4.6 SYSTEM INTEGRATION

As services and technologies evolve, new software and hardware will need to be incorporated into the existing baseline as determined by the applicable Government agent. In addition new security measures will be developed, issued, and require implementation therefore need to be integrated into existing baselines. The Contractor shall:

- Test and evaluate commercial-off-the-shelf applications, Government-off-the-shelf applications and hardware for integration into the C4 networks
- Ensure compatibility with current baseline, resolving conflicts as they arise
- Apply appropriate security measures (STIGs, IAVMs, Tasking Order Compliance…etc) to lock down the application/hardware
- Develop deployment procedures (i.e. package software, installation instructions…etc)
- Have Information Assurance review and sign-off acceptability prior to deployment
- Test and evaluate IA directed patches for compatibility with the current baseline and resolve any conflicts prior to deployment

C.5.3.4.7 ENTERPRISE ENGINEERING

The Contractor shall provide System Engineering services for complex, large-scale, and/or enterprise-type projects. This support shall include:

- Participate in systems engineering planning activities. Provide feedback to both short-range and long-range planning activities to enhance performance and improve efficiency.
- Provide emerging communications and information technology engineering support and technical solutions to improve overall service delivery to include customer support, network, services, proactive system support, etc.
- Develop Cost Benefit Analysis documentation in support of new technology or processes
- Provide design and engineering support for new network and system implementations and upgrades to include hardware, software, projection systems, video switching hardware, video teleconferencing, and other systems to meet project requirements
- Support the Customer's efforts to share and distribute information by electronic means
- Engineer, install, operate and maintain a test lab in support of AFRICOM C4 networks.
- Provide effective technical solutions to complex problems to include Tier 3 troubleshooting of incidents or problems when requested

C.5.3.5 INFORMATION ASSURANCE SERVICES

The Contractor shall assist AFRICOM with the implementation of IA strategies for all supported networks consistent with DoD and National Security Agency (NSA) guidance. The Contractor shall provide services and support to ensure the confidentially, integrity and availability of AFRICOM accredited C4 networks. AFRICOM requires all C4 networks be protected from network attacks, unauthorized access, service interruption and unauthorized disclosure or modification of information that is processed on them.

AFRICOM requires the Contractor to manage the Certification and Accreditation functions; to perform Compliancy functions (patching and VMS), as described below, for assigned servers only, and Architecture and Engineering functions for assigned engineering projects only.

Information Assurance is highly regulatory in nature and strict adherence to the DOD directives listed in the Attachment A - Specific Governing Documents, as well as AFRICOM's instruction, policies, and procedures is required. Several tasks described below referencing "when directed" means that the Contractor shall take direction from AFRICOM's Designated Approval Authority (DAA)/Authorizing Official (AO), AFRICOM's Information Assurance Manager (IAM), EOC DAA/AO and others as designated in writing by the DAA/AO/IAM.

C.5.3.5.1 CERTIFICATION AND ACCREDITATION (C&A)

The Contractor shall provide the following support and services:

- Manage and maintain the Certification and Accreditation (C&A) program for communications and information systems under the purview of HQ AFRICOM
- Prepare and maintain DoD Information Assurance Certification and Accreditation Process (DIACAP) or Risk Management Framework (RMF) artifacts/packages (e.g. Configuration Management Plan, Vulnerability Management Plan, System Plan of Action and Milestones, IT Continuity Plan, Security Design Management Process, Security Requirements Traceability Matrix…etc.) i.a.w. applicable Government directives and policies.
- Develop and maintain C&A documentations including Program of Record (POR) and Program Managed Systems for SIPRNet and NIPRNet connection approval processes
- Validate accreditation worthiness by performing vulnerability scans and DISA STIG checks
- Prepare and maintain Risk Management Framework artifacts/packages when required or directed
- Maintain a copy of all network documentation to include DIACAP or RMF packages, network diagrams, IP ranges, COOP and disaster recovery plans, and the number of systems by type
- Ensure C&A documentation is populated and maintained in the appropriate SIPRNET or NIPRNET Enterprise Mission Assurance Support System (eMASS)
- Ensure systems are established and maintained in accordance applicable C&A directives to include being compliant with the IA Controls and/or RMF Controls assigned by the specified MAC levels
- Serve as Information Assurance point of contact for new, replacement, trial, or test equipment or software being brought into the purview of the AFRICOM accreditation boundary. Ensure the sponsor and/or action officer provides necessary accreditation documentation before fielding, demonstrating or testing the product.
- Evaluate the security risks and provide recommendations on requests to add software and hardware to the Approved Product List
- Integrate with the Change Management process ensuring:
    - Systems have approval to connect or operate

  - The required change has met all security requirements
  - All C&A documentation impacted by the change is updated
- Perform on-site IA C&A assessments on AFRICOM networks and systems at the direction of the Government. [*Note: DoD directives require that approximately 33% of the packages must be assessed each year*]
- Provide support to the AFRICOM Cross Domain Solution program/office.
- Assist, develop, and recommend corrective courses of action for findings identified during network readiness assessments, vulnerability scans and certification and accreditation reviews. For findings directly associated with C&A documentation and processes resolve open security vulnerabilities, focusing on the most critical vulnerabilities first.
- Maintain Information Assurance tools/systems required to support C&A functions when required or directed
- Review, provide input, and (with Government) respond to internal and external taskings

C.5.3.5.2 INFORMATION ASSURANCE COMPLIANCY

The Contractor shall provide the following support and services:

- Implement all applicable Information Assurance Vulnerabilities, Bulletins and Technical Advisories i.a.w. CYBERCOM directives. Report IAVM compliancy; track CYBERCOM Command Tasking Orders (CTOs), FRAGOs, INFOCON; Coordinated Alert Messages (CAMs), and other directives for assigned AFRICOM network assets through the Vulnerability Management System (VMS) or as otherwise directed by CYBERCOM.
- Populate assets and maintain security vulnerability compliancy through the VMS for assigned AFRICOM assets and Program of Record systems.

C.5.3.5.3 INFORMATION ASSURANCE ARCHITECTURE AND ENGINEERING

The Contractor shall provide the following support and services:

- Conduct security engineering reviews and recommendations for increased protection on all assigned hardware, including POR systems. This includes, but is not limited to new and existing projects, capabilities, configurations, testing, and accredited or proposed systems.
- Define requirements or objectives to be met and recommend solutions for an acceptable level of accreditation for the AFRICOM DAA/AO or IAM on POR systems that do not meet an accredited standard.
- Provide technical security reviews and recommendations on all assigned software and hardware products/systems. This includes, but is not limited to information assurance tools, network tools, existing baseline software builds, and new proposed solutions across the enterprise; or based on an approved new requirement.
- Ensure all engineering designs maintain compliance with DOD and Joint Staff directives and policies as well as CYBERCOM orders.
- Assist the Government with ensuring the network architecture plan is documented and an acceptable risk decision is provided to the DAA/AO on the existing and changed configurations.

C.5.3.6 LOGISTICS MANAGEMENT

C.5.3.6.1 CONFIGURATION MANAGEMENT

The Contractor shall follow 5th Signal Command's Configuration Management Plan, processes, and procedures providing configuration management of the AFRICOM C4 networks and systems. The Contractor is a participant and not the process owner.

C.5.3.6.2 SUBSCRIPTION (Software Maintenance) MANAGEMENT SERVICES

Given the software maintenance agreements that AFRICOM (vice 5SC) requires, the Contractor shall track and manage the agreements by:

- Maintaining an up-to-date, Government accessible listing or database of all software maintenance agreements to include at a minimum product name, quantity, cost, agreement start/end dates, and expiration date
- Making best value recommendations about the continuation of maintenance agreements to include consolidating like products with different expiration dates
- Determining the most cost effective approach to renew the agreements
- Notifying the Government at least 90-days prior to the agreement's expiration
- Track all software procurements executed by the contractor and provide report as requested by the Government *[The tracking/reporting of software purchases is also a requirement of the Tools Purchases function --- this is not intended to be duplicative.]*

[Note: The above scope also applies to the CLDJ-HOA software that falls under AFRICOM purview.]

C.5.3.6.3 STANDARD DESKTOP CONFIGURATION MANAGEMENT

The Contractor shall use the 5th Signal approved and managed Standard Desktop Configuration in their maintenance actions. The Standard Desktop Configuration (SDC) will be managed by the 5SC Change Advisory Boards (CAB) with representation from AFRICOM.

The Standard Desktop Configuration is comprised of the desktop Operating System (OS), core applications (e.g., Microsoft Office Suite, Java, Adobe Reader, and anti-virus), as well as HW specific configuration items and the associated configuration characteristics for a specific workstation platform. Changes to the SDC occur when 1) specific SDC components are updated; 2) new components are added to the SDC; 3) security patches are applied to the components in the SDC; or, 4) existing SDC components are retired and removed from the SDC.

C.5.3.6.4 ASSET MANAGEMENT

The Contractor shall maintain AFRICOM's inventory of spare equipment to include Property Book items and other IT supplies such as operating stock and/or bench stock. The Contractor shall establish, follow and manage all communications and IT assets throughout all aspects and phases of the life-cycle. The Contractor shall propose processes, tools and procedures in order to accomplish this. The Government shall approve the formal Asset Management process, procedures and tools to be used. The Contractor shall administer this program and account for all communications and IT assets for AFRICOM in support of the appropriate Government responsible agent. The Contractor shall:

- Perform Property Book /Hand Receipt Holder duties, inventory management, and accountability functions for all network and end user data, voice, VTC and wireless equipment under their control
- Perform receiving, storage, staging, distribution, and turn-in functions for data, voice, VTC and wireless equipment (network and end-user)
- Identify and report to the government equipment that is either lost or damaged beyond economical repair.
- When directed, assist in demilitarizing and disposing of HW and SW at cleared Government facilities i.a.w. applicable DOD guidance.
- Identify and report to the government any excess or end of life equipment

- Ensure resources (stock) that the Government already owns are employed before purchasing new additional items
- Identify and implement best practices and technologies for an effective asset management program
- Track and account for storage media (e.g. hard drives, backup tapes) that process and store NATO SECRET information in accordance C-M (2002)49, "NATO Security Policy". AFRICOM SIPRNet is classified up to U.S. SECRET and NATO SECRET

C.5.4 EUCOM REQUIREMENTS

The Contractor shall provide **dedicated resources** to deliver these requirements. A dedicated resource means EUCOM will fund the full cost of the employee to include staffing-related Other Direct Costs therefore expects all of the resource's basic labor hours to be spent on EUCOM work.

C.5.4.1 CUSTOMER END USER SUPPORT SERVICES

The Contractor shall provide technical support to end users to include:

- Responding to user telephonic and electronic service requests for assistance
- Extending services to support real world operations and exercises
- Managing of user accounts and SIPR/Alternate Tokens
- Providing dedicated end user service technicians when specified by the Government

C.5.4.1.1 EUCOM SERVICE CENTER

The Contractor shall provide Service Center support for EUCOM networks. The Service Center shall be a single point of contact to all supported EUCOM customers for their IT needs. The EUCOM Service Center shall be staffed, as a minimum, during normal work days from 0600 to 1800. Outside of these hours their duties may be transferred to other on-site contractor personnel with approval of the TPOC. Service Center support shall consist of:

- Documenting and tracking user problems (incidents) and service requests until resolution
- Providing incident triage to include resolution when possible and re-assigning or escalating incidents for resolution to other technicians as necessary
- Contacting other service provides (i.e. 5SC CSD, DISA…etc) when necessary to coordinate and resolve incidents and requests
- Notifying the TPOC and other specified Government personnel of all Maintenance Priority 1 and 2 outages within established timeframes
- Contacting on-call personnel when required
- Monitoring the supported C4 networks for circuit/equipment outages, system and software problems…etc.
- Using the Government designated IT event tracking system
  - o *Note: EUCOM currently uses a stand alone, Contractor maintained, Remedy solution*
- Verifying resolution with the end user prior to closing incidents, problems, and requests

C.5.4.1.2 ACCOUNTS MANAGEMENT

The Contractor shall provide consolidated account management service which provisions and de-provisions IT systems accounts as personnel are assigned or depart. Account management services shall include as a minimum:

- Account creation/deletion
- Updating of GAL information

- Issuance and management of User Agreements

C.5.4.1.3 PKI TOKEN SERVICES

The Contractor shall provide Enhanced Trusted Agent (ETA) services as the PRIME provider for EUCOM during normal work hours. It is expected that the majority service required will be on a walk in basis. Token services shall include as a minimum:

- Train and certify sufficient staff to provide continuous service during normal work hours
- Troubleshooting and resolving Token Card failures to include PIN resets
- Requesting certificates for new or reconstituted cards from the Local Registration Authority
- Printing and issuance of cards
- Revoking tokens when required

C.5.4.1.4 REMOTE AND DESKSIDE SUPPORT SERVICES

The Contractor shall provide end user support consisting of remote services and/or deskside support in response to end user requests for assistance. The Contractor shall perform a wide variety of duties to include hardware and software incident troubleshooting and repair; fulfillment of approved service request and upgrades; and troubleshooting of peripheral devices.

C.5.4.1.5 NON-PERMANENT REMOTE CONNECTIVITY AND MOBILE COMMUNICATIONS

The Contractor shall provide Systems Analysis, System Engineering, Systems Security and System Administration services to remote and dial-in EUCOM users in support of EUCOM C4 LANs to include the following:

- Provide IT support to deployed and TDY EUCOM users who are on existing supported networks and systems.
- Provide required support to dial-in EUCOM LNOs.
- Provide a laptop library system to provide for the short-term IT needs of mobile or deployed users.
- Provide support for encrypted disk security configurations for mobile laptops and remote workstations.
- Provide support for mobile computing device implementations (e.g., tablets and smart phones).

The Contractor shall provide Systems Analysis, Systems Engineering, Information Assurance, System Administration, and end-user support services for mobile communications.

C.5.4.1.6 COALITION NETWORK END USER SUPPORT

The Contractor shall provide support for Coalition network systems i.a.w. the requirements for communications and IT support as described in this document for the SLAN network system. The Contractor shall perform an analysis of available technologies that support Coalition objectives. This analysis shall consider the following goals when determining whether or not a new technology should be integrated into the architecture:

- Implement security and IA processes.
- Systems that increase the ability of a member nation to effectively hand over operations to another member.
- Improve availability.
- Improve remote site IA policies and practices.
- Increase user capability.
- Increase ability to hand over operations between member nations.

- Increase interoperability between member nations.
- Reduce footprint.
- Reduce cost.
- Mitigate classified message incidents (CMIs, sometimes referred to as data spills) in the event of an IA breach.

C.5.4.2 EUCOM NETWORK SERVICES

The Contractor shall provide Network Management Services to include those hardware and software standards, solutions, processes, and services which encompass:

- HQ EUCOM C4 networks shown in Attachment C, entitled "USEUCOM C4 Systems Overview"
- SHAPE, Pentagon, and other Stuttgart-area extensions to the HQ EUCOM networks
- Maintaining and providing EUCOM network connectivity by networks and systems to ensure mission critical systems and operations are available with the goal of achieving Government established monthly availability rates, not including authorized or planned service interruptions or preventive maintenance
- Installing, configuring, and maintaining the installed network management systems
- Monitoring the operational status and posture
- Supporting Fault identification and management; and Fault recovery
- Troubleshooting and correcting all network faults to maintain the operational status in a normal, continuously operational state
- Providing Trending and Capacity Planning services to analyze and plan for the efficient utilization and management of the networks
- Providing recommendations on enhancing performance and correcting problems as required
- Supporting service level reporting and submitting logs, statistics, or analytical data, as requested by the Government
- Planning, scheduling, and implementing maintenance actions to sustain the operational viability of the networks, to include forecasting, planning, and supporting technology refreshment /insertion projects
- Install, configure, and maintain secure data devices and associated access control lists for remote access to networks and communications networks

C.5.4.3 STORAGE CAPACITY PLANNING

The Contractor shall assist the Government in establishing the necessary physical and virtual storage to host and retain data for purposes such as content staging, continuity of operations or archival. The Contractor shall assist the Government in identifying and matching the capacity of the IT services and infrastructure to the current and future identified needs of the business. The Contractor shall assist the Government in establishing a framework that covers a range of component capacities and the design/deployment of capacity in order to meet expectations of data collection and analysis for infrastructure utilization and performance. The Contractor shall perform assessments as to whether there are potential problems and issues that must be addressed, and provide the results to the Government. The Contractor shall provide the following storage capacity planning:

- Ensure that cost-justifiable IT capacity always exists and is matched to the current and future identified needs of the business.
- Accommodate scalability requirements.
- Avoid incidents caused by lack of capacity.

The Contractor shall consider the following elements for all Storage Capacity Planning:

- Reliability - the time for which a component can be expected to perform under specific conditions without failure.
- Scalability - the ability to expand network storage capacity, often utilizing an appliance to easily add storage and track storage growth to organization growth.
- Flexibility - the ability to add applications (e-mail, databases) to the networked storage; flexibility can be added by using a device that can handle application storage or share files.

C.5.4.3.1 BACK-UP AND RECOVERY

The Contractor shall develop, document and implement a comprehensive backup and recovery plan to include:

- Assessment plan
- Design plan
- Implementation plan
- Verification, testing, and reporting

C.5.4.4 REMOTE EXTENSIONS – PERMANENT REMOTE SITES

The Contractor shall provide connectivity and IT end-user support services for Permanent Remote Sites to include:

- Sites that are not physically co-located with the core command network
- Supporting multiple users at the remote site (as opposed to individual quarters connectivity
- Sites that are intended to remain in the same location for an extended period of time, usually in the order of years.

C.5.4.4.1 SUPREME HEADQUARTERS ALLIED POWERS EUROPE (SHAPE)

The Contractor shall provide Systems Analysis, Systems Engineering, Information Assurance and System Administration services to remote extensions to the supported C4 LANs. The scope covers support for the Supreme Allied Commander Europe (SACEUR) Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium (in support of the HQ EUCOM C4 LANs). The Government will require permanent support at this location to provide systems administration and server support for EUCOM staff located at SHAPE, as well as temporary travel to this site on occasion for server upgrade and firewall support. Contractor employees providing these services are part of the U.S. Civilian Component and as shall fall under (be eligible for) Status of Forces Agreement (SOFA) status in Belgium. The Contractor shall provide the following services:

- Provide an operational ULAN/SLAN and connection to the SIPRNet/NIPRNet and common network services (to include email, shared file storage, network printing, domain name service, internet protocol address management);
- Provide audiovisual/VTC support as required (such as Tandberg desktop VTC);
- Provide Very Important Person (VIP) level service for C4 Systems specified VIPs; VIP requests are prioritized “URGENT”.
- Configure and administer end-user workstations i.a.w. HQ EUCOM standards;
- Provide hardware maintenance on workstations, printers, and network equipment installed in the facility;
- Assist in the preparation and maintenance of accreditation documentation for the networks in the facility and oversee security of the networks;
- Provide GCCS (and GCCS variant) administration;
- Be responsible for property accountability of communications, network, and network-related cryptographic devices;

- Provide support for communications connectivity to the various networks, to include satellite communications, communications security, and related infrastructure;
- Provide informal over-the-shoulder user training as required; and
- Provide preventative maintenance for systems and equipment i.a.w. approved PMI schedules.

C.5.4.4.2 OFFICE OF DEFENSE COOPERATION (ODC) SITES TO INCLUDE AFFILIATE SITES

The Contractor shall provide Systems Analysis, Systems Engineering, Information Assurance, System Administration, connectivity, and end-user support services for U.S. government and industry participation/activities in foreign nation defense initiatives. ODC sites typically provide significant challenges for connectivity since they are often located in countries with unreliable/unstable infrastructures and governments.

The Contractor shall assist the Government in performing assessments of each site to determine which solution is the most effective at meeting the site requirements. Each ODC site must be provided with service i.a.w. its size and service requirements since some sites will require significantly more throughput and support than others. Supported networks shall consist of ULAN and SLAN and are implemented via cryptographic devices and routing technologies. ODC site connectivity can be achieved by utilizing satellite networks, host nation networks, or existing Embassy networks if co-located with the Embassy.

The Contractor shall provide support services tailored for remote users including Tier I-III phone and e-mail support, network-based remote desktop support, and maintain a knowledge base of remote support solutions. For ODC sites receiving their IT services from the Dept of State the Contractor shall act mainly as the ODC's technical advocate providing solutions allowing the integration of DOD applications into the DOS enterprise. Deploying IT technicians must have a broad skill set to support all devices at a location in order to achieve maximum value from a minimum number of technicians.

EUCOM currently has 38 ODC sites, 18 of which receive their primary IT support services from the Department of State. In addition, there currently are 19 sites affiliated with EUCOM requiring support. The number of affiliated sites may increase in the future.. Supported networks shall consist of EUCOM ULAN and SLAN networks implemented via cryptographic devices and routing technologies. Upon Government direction, technician(s) will travel to remote sites to support workstations, servers, routers, switches, smart phones, notebooks and VTC systems. Each site will need to be visited annually to provide on-site support and tech refresh.

C.5.4.4.3 CONNECTIVITY TO INTERAGENCY PARTNERS AND US EMBASSIES

The Contractor shall implement a Government-approved overall Command architecture and means for users to communicate with Interagency Partners and US Embassies.

C.5.4.4.4 RESIDENTIAL NETWORK CONNECTIVITY

The Contractor shall provide Systems Analysis, Systems Engineering, System Administration, Information Assurance, connectivity, and end-user support services for communications and IT for designated residential network access capability. The Contractor shall follow the approved EUCOM processes and procedures for the identification, installation and support of all communications and IT capabilities in residences.

C.5.4.5 VISUAL INFORMATION AND PRESENTATION SERVICES SUPPORT

The Contractor shall provide support for EUCOM Visual Information and presentation services. These systems include, but are not necessarily limited to, the following:

- Defense Information Systems Network (DISN) Video Services (DVS) Video Teleconferencing (VTC) Facilities;
- ULAN, IP-based and ISDN VTC Systems
- SLAN, IP-based, and dial-up VTC Systems;
- Collaborative Tools requiring video capabilities;
- Portable or other mobile VTC capabilities
- Net-Centric Enterprise Services (NCES).
- Secure desktop video phone device.
- MCU Bridge (Tandberg or similar).
- CODECS (Tandberg 2500s or similar).
- Desktop VTC equipment
- Unified Communications
- IPTV

The Contractor shall:

- Perform VTC scheduling and manage Command assets used for scheduling and bridging VTC events.
- Coordinate reservation and scheduling of VTC services with outside agencies when required.
- Perform VTC set up and operations, multi-session bridging, and other related administrative tasks in order to enable VTC connectivity both with internal and external participants. The scope of this support includes but is not limited to assisting end users in operating equipment and in establishing, maintaining and troubleshooting VTC connectivity throughout the duration of the video-conferencing session.
- Support both point-to-point and simultaneous point-to-multi-point connections.
- Provide remedial and preventative maintenance, hardware integration of comparable components,
- Provide user and operator level training, management of user accounts, and develop and maintain system documentation for systems.
- Perform remote diagnostics in order to maintain, restore or otherwise establish connectivity.
- Maintain a record of all VTC operations and provide a VTC Usage Report to the government.
- Provide, when directed, Presentation services and support for critical users in the areas of broadcast communications, to include singular events and/or collaborative on-line events.
- Provide dedicated in-room support for all General Officer VTCs held in the Headquarters' Conference Room (HCR) in Building 2314. Services to include:
  - Set-up and sound checks prior to the conference
  - Remain in the HCR (or in the immediate area, as requested) to monitor VTC performance during the event
  - Support other scheduled VTCs upon request during normal duty hours and with 24-hours' notice outside of normal duty hours

C.5.4.5.1 EUCOM MISSION COMMAND CENTER (EMCC) PRESENTATION SERVICES

The Contractor shall provide O&M for EMCC's virtual device management systems and audio visual systems provided through the Thinklogical Audio/Visual equipment suite.

The EMCC consists of key operational rooms, including Joint Operations Center (JOC), Senior Decision Cell (SDC), and the Focal Point Operations Center (FPOC). The JOC also contains 5 PODs in the JOC that can operate at multiple classifications levels and 1 NON-Class POD for special internet access. Additionally, the Headquarters Conference Room and the Joint Network Operational Center are tied into the EMCC Master ThinkLogical Matrix Routing System.

[Note: Reference PWS Attachment C for EMCC Thinklogic Details.]

The Contractor shall:

- Provide O&M support, coordination, and monitoring for all systems related work in the EMCC, including Audio Video (AV) routing matrix, computer systems, architecture, controlled lighting.
- Provide user training and over-the shoulder guidance for all EMCC personnel to ensure operational efficiency to include creating TTPs, SOPs and operational guides, as required.
- Create and follow a Preventative Maintenance Schedule (PMS) to maintain and prolong equipment lifecycles to include bulb replacements.
- Develop systems stress tests and implement them in coordination with EMCC exercises.
- Provide a post exercise report with system reliability and performance details to include fix actions implemented or recommendations to mitigate future problems
- Provide weekly status briefs to EMCC/J3 leadership on the EMCC systems and project status.
- provide O&M for EMCC's virtual device management systems and audio visual

C.5.4.6 CRYPTOGRAPHIC EQUIPMENT SUPPORT SERVICES

The Contractor shall perform cryptograhic equipment support services i.a.w. COMSEC Material Direct Support Activity (CMDSA) user account guidelines and training. Procurement of most items associated with cryptographic equipment remains an inherently governmental responsibility. The Contractor shall provide cryptographic equipment support to include:

- Maintain accountability of cryptographic keying material i.a.w. governing regulations
- Install, configure, maintain, and re-key encryption devices as necessary to support continuous operations
- Configure and maintain access control lists for remote access to networks

C.5.4.7 COMMAND AND CONTROL SYSTEMS, APPLICATIONS AND SERVICES

The Contractor shall provide C2 systems applications and services support for EUCOM in the areas of systems engineering; server configuration; software engineering; and display management. This support is limited what is allowable by Global Command and Control System - Joint (GCCS-J) Program Management Office (PMO). In addition, this PWS is intended to provide O&M services as it relates to IT and not Operator Services (such as Common Operating Picture management).

EUCOM has 3 instances of GCCS-J requiring support; EUCOM, USBICES, and SEAGULL. The Contractor shall provide the following command and control systems support:

- Procurement of hardware with minimum specifications as determined by the PMO and GOTS developer.
- Proposed device connectivity as determined by the PMO and GOTS developer.
- Proposed rack space design for servers with proper cooling systems.
- Installation of GOTS and Government-provided equipment and software that is not proprietary and does not require specialized installation
- System Administration; System Maintenance; Technical Refresh/Upgrade Support

- Provide O&M virtual device management system and audio visual capability provided through Thinklogical architecture.

C.5.4.8 SYSTEM ENGINEERING SUPPORT

The Contractor shall provide Network and System Engineering Support services to improve customer service, system performance, and reliability for the C4 Networks and Systems on the EUCOM and Coalition (CENTRIXS and SEAGULL) networks.

C.5.4.8.1 REQUIREMENTS ANALYSIS

The Contractor shall assist the Government in assessing system performance, planning for new and evolving C4 systems, evaluating proposals for the migration of existing functionality, and making recommendations for corrections and enhancements. Contractor planning services shall include providing draft documentation and technical input to documentation for assessments, plans, system implementations and architectures, and engineering designs related to new, evolving, and existing C4 systems. At the direction of the Government the Contractor shall conduct and/or participate in strategic planning, studies, and evaluations to provide resource requirements, present recommended solutions, determine labor and tools estimates, and plan/refine schedules. The Contractor's effort shall include:

- Providing technical studies, reviewing plans, evaluating state of the technologies prior to fielding of new releases or systems
- Reviewing C4 plans and policies and providing observations and questions for consolidated responses
- Researching and coordinating technical issues and requirements and drafting new and updated policy governing technical issues
- Providing technical analyses and draft reports of C4 system tests, assessments, and architectures
- The Contractor shall participate in meetings as required by the Government to include attending conferences; technical interchange seminars; interoperability meetings; and Government briefings related to integration, migrations, and maintenance of C2, coalition, and bi-lateral system architectures

As directed by the Government, the Contractor shall perform analysis, provide recommendations, and prepare and provide planning documentation for Government approval for the transition plan of current services into the JEN/JIE environment.

C.5.4.8.2 SYSTEM INTEGRATION

As services and technologies evolve, new software and hardware will need to be incorporated into the existing baseline as determined by the applicable Government agent. In addition new security measures will be developed, issued, and require implementation therefore nrmd to be integrated into existing baselines. The Contractor's effort shall include:

- Test and evaluate commercial-off-the-shelf applications, Government-off-the-shelf applications and hardware for integration into the C4 networks
- Ensure compatibility with current baseline resolving conflicts as they arise
- Apply appropriate security measures (STIGs, IAVMs, Tasking Order Compliance…etc) to lock down the application/hardware
- Develop deployment procedures (i.e. package software, installation instructions…etc)
- Have Information Assurance review and sign-off acceptability prior to deployment
- Test and evaluate IA directed patches for compatibility with the current baseline and resolve any conflicts prior to deployment

C.5.4.8.3 NETWORK ENTERPRISE ENGINEERING

The Contractor shall provide System Engineering services for complex, large-scale, and/or enterprise-type projects. This support shall include:

- Participate in systems engineering planning activities. Provide feedback to both short-range and long-range planning activities to enhance performance and improve efficiency.
- Provide emerging communications and information technology engineering support and technical solutions to improve overall service delivery to include customer support, network, services, proactive system support, etc.
- Develop Cost Benefit Analysis documentation in support of new technology or processes
- Provide design and engineering support for new network and system implementations and upgrades to include hardware, software, projection systems, video switching hardware, video teleconferencing, and other systems to meet project requirements
- Support the Customer's efforts to share and distribute information by electronic means
- Provide effective technical solutions to complex problems to include Tier 3 troubleshooting of O&M problems when requested

C.5.4.8.4 Project Management (PM)Support

The Contractor shall provide centralized project management support to integrate, monitor and control interdependencies among assigned EUCOM projects. The Contractor may or may not have full control of the Engineering projects they are assigned. Depending upon the scope, size, complexity, and Government needs, the Contractor may be a member of an integrated project management team consisting of both Government and other Contractors. The Project Charter shall clearly identify the CITSII Contractor's roles and responsibilities for the particular project.

The Contractor shall ensure that activities and processes are coordinated and integrated i.a.w. 5SC's documented processes (when they exist) or sound PMI framework (when they don't). As needed, these processes include applying an integrated, standards-based project management approach lifecycle to:

- Balance competing constraints of scope, quality, schedule; budget, resources, and risk while satisfying project requirements and addressing stakeholder expectations
- Define and manage project management processes, project schedule, quality standards, measures and metrics, document configuration management; change management, and tracking risks and issues

Specific Project Management support to lead the planning and implementation of projects shall include:

- Facilitating the definition of project scope, goals and deliverables through interaction with the stakeholders/customers in requirements gathering meetings.
- Developing Project Charter, Scope Document, and Requirements document as need to satisfy project needs
- Developing a Project Plan, for Government review and approval, that defines as a minimum the: scope, goals, deliverables, schedule/milestones, resource requirements, and work breakdown structure (WBS) identifying project tasks.
- Managing the project, tracking project deliverables and materials to facilitate completion of the work on time and within the established budget.
- Reporting status to stakeholders.

This task while being performance based shall have a limited level of level of effort equal to 3 dedicated FTEs.

C.5.4.9 INFORMATION ASSURANCE SERVICES

The Contractor shall implement IA strategies for the EUCOM Networks consistent with DoD and National Security Agency (NSA) guidance. The Contractor shall provide services and support to ensure the confidentially, integrity and availability of EUCOM accredited C4 networks. EUCOM require all C4 networks be protected from network attacks, unauthorized access, service interruption and unauthorized disclosure or modification of information that is processed on them. The Contractor will research, develop and implement a holistic risk management strategy for C4 networks to enable the execution of EUCOM operations.

Information Assurance is highly regulatory in nature and strict adherence to the DOD directives listed in the Attachment A - Specific Governing Documents as well as EUOM's instruction, policies, and procedures is required. Several tasks described below referencing "when directed"; the Contractor shall take direction from EUCOM's DAA/AO, EUCOM's IAM and others as designated in writing.

C.5.4.9.1 INFORMATION ASSURANCE PROGRAM MANAGEMENT

The Contractor shall provide the following support and services:

- Implement and manage the EUCOM network security policy.
- Manage and maintain the Certification and Accreditation (C&A) program for communications and information systems under the purview of HQ EUCOM.
- Prepare for, assist with, and monitor IA assessments (network readiness assessments, DISA Security Readiness Reviews (SRR), Command Cyber Readiness Inspections, NSA Red and Blue Team assessments, vulnerability scans, certification and accreditation reviews) for EUCOM. Develop and/or implement corrective courses of action for findings identified during these assessments. Resolve open security vulnerabilities in a timely manner focusing on most critical vulnerabilities first.
- Ensure all internal (CITS Contractor) personnel granted elevated privileges or performing IA functions on EUCOM systems/networks are trained and certified i.a.w. the DoD Manual 8570.01M, Information Assurance Workforce Improvement Program.
- Maximize use of external organizational reciprocity agreements in support of DIACAP compliancy.
- Integrate information assurance and security principles in the Change Management process in the design and development phase.
- Develop technical standards (SOP/TTPs, technical implementation instructions, or other required documentation) for security devices, security operations and other operations as required for Government approval. Ensure all technical standards are updated, maintained, and centrally located for distribution as needed.

C.5.4.9.2 CERTIFICATION AND ACCREDITATION (C&A)

The Contractor shall provide the following support and services:

- Serve as Information Assurance point of contact for promotional, test, new, replacement and/or Contractor equipment being brought into the purview of the EUCOM accreditation boundary. Once this equipment is identified, ensure the system/program managers provide proper accreditation documentation and make necessary changes/additions to the EUCOM DIACAP packages.
- Develop and maintain C&A documentations (including Program of Record (POR) and Program Managed Systems) for SIPRNet and NIPRNet connection approval processes.

- Maintain a copy of all network documentation. This includes, but is not limited to DIACAP packages, network diagrams, IP ranges, COOP and disaster recovery plans, and the number of systems by type.
- Prepare and maintain DIACAP or RMF artifacts/packages (e.g. Configuration Management Plan, Vulnerability Management Plan, System Plan of Action and Milestones, IT Continuity Plan, Security Design Management Process, Security Requirements Traceability Matrix and other documentation to satisfy DoDI 8500.2 IA controls i.a.w. DoD 8510.01 and EUCOM directives, policies and SOPs.
- Perform on-site IA C&A assessments (e.g. IA Control Validation) on EUCOM networks and systems.
- Ensure C&A documentation is populated and maintained in the appropriate SIPRNET or NIPRNET Enterprise Mission Assurance Support System (eMASS)
- Review and with Government approval provide input to internal and external taskings.

C.5.4.9.3 COMPUTER NETWORK DEFENSE (CND)

EUCOM CND requirements encompass SIPR, NIPR, and Coalition networks, as specified below:

EUCOM SIPR AND NIPR CND REQUIREMENTS:

The Contractor shall provide the following support and services:

- Develop and recommend internal procedures for handling network related incidents and protecting EUCOM networks.
- Archive and audit security event logs i.a.w. DoD policy, and if applicable NATO security policy.
- Implement measures to prevent unauthorized software from being installed and executed on EUCOM systems (current IA tool – Bit9).
- Report, mitigate and/or resolve all classified security incidents (e.g. data spills) that impact EUCOM networks within time constraints identified by applicable directive.
- Maintain Information Assurance tools systems (limited to firewalls, encryption tools, Vulnerability Scanning systems, Security Information Management system, Content Filtering, application and device control systems) residing on the EUCOM networks. Ensure all changes to Information Assurance network security devices (firewalls.) are submitted to and approved by the HQ EUCOM CAB/CCB.
- Upon request provide necessary information (e.g. firewall logs, system logs, etc.) to the Tier III Computer Network Service Provider(s) and other designated organizations in the performance of forensic analysis and law enforcement.

EUCOM COALITION CND REQUIREMENTS:

The Contractor shall provide the following support and services:

- Take appropriate measures to respond to known and possible network attacks i.a.w. applicable DoD policies, directives and instructions.
- Develop and recommend internal policies and procedures for handling network related incidents and protecting networks.
- Archive and audit security event logs i.a.w. DoD policy, and if applicable NATO security policy.
- Implement measures to prevent unauthorized software from being installed and executed on systems.
- Archive and review system audit logs and all other pertinent log files that will support incident response activities.

- Report, mitigate and/or resolve all classified security incidents (e.g. data spills) that impact networks within time constraints identified by applicable directive.
- Ensure the installation and support of Host Based Security System (HBSS) meets all CYBERCOM requirements and timelines. Monitor HBSS; ensure anti-virus definitions are updated; unmanaged hosts are tracked/remediated; evaluate/mitigate any discrepancies.
- Monitor, report, mitigate and/or resolve all network anomalies (e.g. unauthorized network access, etc.) that occur on assigned networks.
- Develop and manage incident response actions (e.g. Tactics, Techniques and Procedures)
- Support incident reporting activities i.a.w. CND Tier 2 policies and directives. Collaborate and interface with external organizations/agencies on security related issues and investigations. Report incidents to the Network Warfare Center (NWC) and DAA/AO.
- Maintain Information Assurance tools systems (i.e.: firewalls, encryption tools, Intrusion Detection Systems, Intrusion Prevention Systems, Vulnerability Scanning systems, Security Information Management system, Content Filtering, Correlation Systems, Malware protection systems, application and device control systems…etc) residing on the EUCOM networks. Ensure all changes to Information Assurance network security devices (e.g. firewalls, IDSs, IPSs, sensors, and HBSS, etc.) are submitted to and approved by the HQ EUCOM CAB/CCB.
- Upon request provide necessary information (e.g. firewall logs, system logs, etc.) to the Tier III Computer Network Service Provider(s) and other designated organizations in the performance of forensic analysis and law enforcement.

C.5.4.9.4 INFORMATION ASSURANCE COMPLIANCY

The Contractor shall provide the following services for EUCOM (to include Coalition networks):

- Support and ensure EUCOM and are compliant with the DoD Information Assurance Vulnerability Management (IAVM) Program
- Evaluate and implement all applicable Information Assurance Vulnerabilities, Bulletins and Technical Advisories i.a.w. CYBERCOM directives. Report IAVM compliancy; track CYBERCOM Command Tasking Orders (CTOs), FRAGOs, INFOCON; Coordinated Alert Messages (CAMs), and other directives for EUCOM network assets through the Vulnerability Management System (VMS). Ensure weekly reports are compiled and sent to the NWC. Perform analysis, implement, and report the compliancy of Information Conditions (INFOCON) changes and Communications Tasking Orders (CTO).
- Populate assets and maintain security vulnerability compliancy through the VMS for EUCOM assets and Program of Record systems.
- Perform vulnerability scans/checks on all EUCOM assets (including POR systems) coordinate vulnerability scans/checks as needed and ensure periodic audits are done using the Gold Disk, Retina, or other DoD approved vulnerability scan tools. Evaluate and ensure security threats are mitigated, remediated or waived i.a.w. accepted time constraints.
- Comply with DoD ports and protocol management program. Track and document approved “opened” ports and protocols inbound and outbound.
- Manage and monitor the IA posture/compliancy of Secret and Below Interoperability (SABI)/ CDS devices for HQ EUCOM.
- Conduct periodic internal audits to ensure compliance of the IA Workforce Improvement Program; resolve discrepancies if found.
- Document and maintain an approved software and hardware baseline for all Information Systems under the purview of EUCOM. This includes, but is not limited to routers, switches, servers, workstations, printers, and digital senders, etc.

C.5.4.9.5 ARCHITECTURE AND ENGINEERING SERVICES

The Contractor shall provide the following support and services:

- Conduct security engineering reviews and recommendations for increased protection on all EUCOM hardware, including POR systems. Includes, but is not limited to new and existing projects, capabilities, configurations, testing, and accredited or proposed systems.
- Define requirements or objectives to be met and recommend solutions for an acceptable level of accreditation for the EUCOM DAA/OA or IAM for POR systems that do not meet an accredited standard.
- Provide technical security reviews and recommendations on all software and hardware. Includes, but is not limited to information assurance tools, network tools, existing baseline software builds, and new proposed solutions across the enterprise; or based on an approved new requirement.
- Provide security reviews and recommendations to enhance the security posture on all existing and proposed enterprise network configurations within the EUCOM accreditation boundary; this also includes approved tunnels and remote connections.
- Ensure the network architecture plan is documented and an acceptable risk decision is provided to the DAA/AO on the existing and changed configurations.

C.5.4.10 LOGISTICS MANAGEMENT

C.5.4.10.1 CONFIGURATION MANAGEMENT

The Contractor shall provide Configuration Management of the EUCOM C4 networks and systems. The Contractor shall implement and maintain a configuration management program that encompasses documented change control procedures and practices for both hardware and software on all supported networks/systems to include coalition. Procedures/practices shall be documented in a Configuration Management Plan submitted for the approval of the Government.

The program shall complement and work in concert with EUCOM CMB and CCB activities. The scope of this work includes:

- Support the activities of the EUCOM Configuration Management Board (CMB) and Configuration Control Board (CCB).
- Record and publish minutes of Configuration Control Board (CCB), and associated Information Resource Management meetings.
- Establish and maintain configuration data for supported communications and IT software and hardware, to include but not be limited to the following:
    - Supported items by type and serial number
    - Maintenance history
    - Warranty information
    - License information.
- Work directly with requesters and technical support personnel to gather sufficient configuration management data
- Ensure proper licensing for software in use on supported systems and networks and maintain a system of licensing accountability and internal control procedures.
- Make recommendations for communications and IT system improvements that result in optimal hardware and software usage.

The Contractor shall ensure proper CM of the EUCOM communications, IT, and C4 networks, to include, but not be limited to, the following:

- Maintain documentation on the configuration of the network and its components to include network architecture diagrams,
- Document all changes to the configuration of the network.
- Document current revision level of all key network components, and
- Maintain all required documentation relating to domain name service, IP addressing, and host naming.
- Maintain inventory of all Data Center, Server, and Network assets

C.5.4.10.2 ASSET MANAGEMENT

The Contractor shall maintain EUCOM's inventory of spare equipment to include Property Book items and other IT supplies such as operating stock and/or bench stock. The Contractor shall establish, follow and manage all communications and IT assets throughout all aspects and phases of the life-cycle. The Contractor shall propose processes, tools and procedures in order to accomplish this. The Government shall approve the formal Asset Management process, procedures and tools to be used. The Contractor shall administer this program and account for all communications and IT assets for EUCOM in support of the appropriate Government responsible agent. The Contractor shall:

- Perform Property Book /Hand Receipt Holder duties, inventory management, and accountability functions for all network and end user data, voice, VTC and wireless equipment under their control
- Perform receiving, storage, staging, and distribution functions for data, voice, VTC and wireless equipment (network and end-user)
- Identify and report to the government equipment that is either lost or damaged beyond economical repair
- Identify and report to the government any excess or end of life equipment
- Ensure resources (stock) that the Government already owns are employed before purchasing new additional items
- Recommend candidate equipment to the government for lifecycle replacement semi-annually or upon Government request
- As directed by the responsible Government agent, turn-in excess or end of life equipment on the Contractor's Property Book
- Identify and implement best practices and technologies for an effective asset management program
- Track and account for storage media (e.g. hard drives, back-up tapes) that process and store NATO SECRET information in accordance C-M (2002)49, "NATO Security Policy". EUCOM SIPRNet is classified up to U.S. SECRET and NATO SECRET

C.5.4.10.3 LICENSE AND SUBSCRIPTION MANAGEMENT SERVICES

The Contractor shall assist the Government in maintaining the license database. The Contractor shall only install Government approved applications or software components on a user's computer. The Contractor shall:

- Install software not normally part of the SDC only as directed by the Government
- Track and report discrepancies between installed software and the license database.
- Identify and request additional licenses as the need is identified.

C.5.4.10.4 STANDARD DESKTOP CONFIGURATION MANAGEMENT

The Contractor shall maintain and manage the Standard Desktop Configuration and implement changes to the SDC i.a.w. the provisions stated in this paragraph.

The standard desktop configuration (SDC) consists of standard software applications and associated components provided to all desktop computer users for each network. The SDC will be managed by the EUCOM Configuration Control Boards (CCBs), with implementation actions carried out by personnel on the Consolidated Help Desk. The Consolidated Help Desk shall receive requests for the addition of new software to the SDC, and shall forward those to the CCB for adjudication/consideration. Upon approval by the Government, the Consolidated Help Desk personnel shall establish and conduct appropriate software testing prior to fielding. If test results are favorable, the application shall be added to the SDC and documented as such.

C.5.4.11 VIRTUAL DESKTOP INFRASTRUCTURE (VDI) O&M SERVICES

The Contractor shall provide Operations and Maintenance support to include applicable IA services for EUCOM's VDI infrastructure for desktop presentation in the SIPRNet security environment. The Contractor shall be responsible for O&M on all servers, storage, applications, and network equipment as identified in Attachment C.14 - EUCOM VDI Diagram and Equipment List. O&M services encompass support for the current Phase 1 VDI server environment, VDI Storage Area Network, VMware View environment as well as user end points connected to the applicable network. These services span other PWS requirements (i.e. system administration, network management, configuration management, information assurance, storage management, etc…) described elsewhere in PWS section C.5 - REQUIRED TASKS and C.5.4 - EUCOM REQUIREMENTS.

C.5.5 HORN OF AFRICA (HOA) REQUIREMENTS IN SUPPORT OF AFRICOM

The Contractor shall provide **dedicated resources** to deliver these requirements. A dedicated resource means that all of the contractor's labor hours are spent supporting these AFRICOM requirements in the Horn of Africa (HOA) region.

Note: Networks and information systems used in HOA are an extension of the AFRICOM IT enterprise.

During Task Order performance, the Government envisions that some service consolidation will occur as the vision for JIE unfolds. As such, the Government may seek contractor recommendations on which services can be consolidated and provided remotely to HOA in the future.

C.5.5.1 CUSTOMER END USER SUPPORT SERVICES

The Contractor shall provide technical support to end users to include:

- Responding to user's telephonic, electronic, and walk-in service requests for assistance
- Extending services to support real world operations and exercises
- Managing of user accounts and SIPR/Alternate Tokens
- Providing dedicated end user service technicians when specified by the Government

C.5.5.1.1 REGIONAL SERVICE DESK SERVICES (HORN OF AFRICA)

The Contractor shall provide Regional Service Desk - Horn of Africa (RSD-HOA) support for designated AFRICOM NIPR, SIPR and Coalition network enclaves in the HOA region. RSD-HOA support includes the ability to manage and coordinate the handling of incidents, problems, and requests with end users and IT groups for unclassified and classified equipment. The RSD-HOA shall be staffed 24/7/365 and provide multiple means (e.g., walk-in, single DSN number and single Web interface) for requesting service. RSD-HOA manages the life cycle of incidents, problems, and service requests including fulfillment, verification, and closure.

The RSD-HOA operates as a satellite of the 5th Signal Command Enterprise Service Desk (ESD). The Contractor's RSD-HOA support shall consist of:

- Document, assess, track, and resolve or fulfill service desk incidents and requests until resolution or closure.
- Servicing walk-in customers. The Contractor can expect a high volume of walk-in customers, established walk-in hours from 0900-1100 and 1300-1500 daily
- Providing incident triage to include resolution when possible and re-assigning or escalating incidents for resolution to other technicians as necessary
- Contacting other service provides (i.e. 5SC ESD, DISA, NCTAMS LANT, etc) when necessary to coordinate and resolve incidents and requests
- Notifying the TPOC, other specified Government personnel, and when possible all affected users of all Maintenance Priority 1 within 30 minutes and Maintenance Priority 2 outages within 1 hour
- Contacting on-call personnel when required
- Monitoring the supported C4 networks for circuit/equipment outages, system and software problems.
- Using the Government designated IT event tracking system currently 5th Signal Command's Remedy-based NetOps Support System (NSS).
- Verifying resolution with the end user prior to closing incidents, problems, and requests
- Upon resolution of an incident for outage of service, provide the Government with written information regarding the reason for the outage, corrective actions taken, and any follow-on actions.
- Input information obtained from addressing Service Desk tickets and from other lessons learned into the NSS Knowledge Repository to support analysis, trouble shooting, and future service delivery
- Provide Service Desk Services for VIP and forward-deployed end users, including support for appropriate services (e.g., remote access, OWA, email, email redirection, client HW, client SW, and deployable process support). *Note, this includes service to:*
  - *Executive VIPs (EVIP) – A subset of VIPs that includes the most senior executives in AFRICOM/CJTF-HOA. EVIPs receive the same level of service as VIPs, but in addition, EVIP end users are provided manual internal notifications [e.g., Situational Reports (SITREPS) and outage notifications].*
  - *Forward-Deployed – End users preparing to deploy to or assigned temporarily to forward operating locations within the defined Combined Joint Operations Area.*

C.5.5.1.2 VIRTUAL DESKTOP INFRASTRUCTURE (VDI) O&M SERVICES

The Contractor shall provide Operations and Maintenance support to include applicable IA services for AFRICOM's VDI infrastructure for desktop presentation in single or multi-level security environments. The Contractor shall be responsible for O&M on all servers, storage, applications, and network equipment as identified in Attachment C - AFRICOM VDI Diagram. O&M services encompass support for the current Phase 1 VDI server environment, VDI Storage Area Network, CITRIX desktop environment as well as user end points connected to the network. These services span other PWS requirements (i.e.

system administration, network management, configuration management, information assurance, storage management …etc) described elsewhere in PWS section C.5 REQUIRED TASKS.

C.5.5.1.3 ACCOUNTS AND IDENTITY MANAGEMENT

The Contractor shall provide consolidated accounts and identity management service which provisions and de-provisions IT system accounts (e.g. end user, systems administrator, group, etc.) as personnel are assigned or depart the Command. Account and identity management services shall, at a minimum, include:

- Account creation with minimum attributes based on the status categories as identified by the Government
- Updating of GAL information
- Issuance and management of User Agreements
- Modify end user accounts including move, add, change, disable and deactivate.
- Provide end user access to AFRICOM workstations based on account and workstation permissions.
- Delete or transfer all network end user data associated with an account no sooner than 30 calendar days after the Government requests account deactivation.
- Provide network end user data associated with an account during the deactivation process, if requested by the Government.
- Operate and maintain a web-based end user reporting tool for account management.
- As required, generate AFRICOM user account reports from Active Directory or the identified identity management solution.
- Perform monthly deactivation of dormant accounts on the network as specified by the Government.
- Perform life cycle event (create, modify, deactivate and delete) management for non-person entity (NPE) accounts such as groups and distribution lists.
- Add or delete groups for assigned Active Directory Organizational Units (OUs), including certain restricted or sensitive groups.
- Change specific attributes of groups, including security permissions.

C.5.5.1.4 PKI TOKEN SERVICES

The Contractor shall provide Enhanced Trusted Agent (ETA) services as the PRIME provider for AFRICOM during normal work hours. It is expected that the majority service required will be on a walk in basis. Token services shall include as a minimum:

- Train and certify sufficient staff to provide continuous service during normal work hours
- Troubleshooting and resolving Token Card failures to include PIN resets
- Requesting certificates for new or reconstituted cards from the Local Registration Authority
- Printing and issuance of cards
- Revoking tokens when required

C.5.5.1.4.1 Local Registration Authority (LRA)

The Contractor shall provide LRA services for the HOA as well as other locations remotely at the direction of HQ Army CIO G6. Training is limited therefore must be schedule well in advance; LRA Training consists of a 2-step process (DOD and Army specific) and is only available in CONUS. A certified LRA shall support the following LRA functions:

- Sourcing, distribution, and installation of user PKI devices
- Identity proofing of certificate applicants for requestors (end users)
- Using the Token Management System to authorize certificate issuance, certificate revocation, suspension, restoration, PIN reset or key recovery
- Transmitting certificates to ETAs when required
- Records shall be maintained IAW directives and turned over to the identified Government agent upon request, removal of requirement, or the end of contract, whichever is sooner

(Note: While this FTE may be used to support other functions his/her LRA duties shall take precedent at all times. Additionally, the Contractor shall ensure all physical security as well as IT administration requirements are followed at all times)

C.5.5.1.4.2 Enhanced Trusted Agent (ETA)

The Contractor shall provide Enhanced Trusted Agent (ETA) services whenever the HOA LRA is not available. It is expected that the majority service required will be on a walk in basis. Token services shall include as a minimum:

- Train and certify sufficient staff to provide continuous service during normal work hours
- Troubleshooting and resolving Token Card failures to include PIN resets
- Requesting certificates for new or reconstituted cards from the Local Registration Authority
- Printing and issuance of cards
- Revoking tokens when required

C.5.5.1.5 REMOTE AND DESKSIDE SUPPORT SERVICES

The Contractor shall provide end user support consisting of remote services and/or deskside support in response to end user requests for assistance. The Contractor shall perform a wide variety of duties to include hardware and software incident troubleshooting and repair; fulfillment of approved service request and upgrades; and troubleshooting of peripheral devices.

C.5.5.1.6 COALITION NETWORK END USER SUPPORT

The Contractor shall provide support for Coalition network systems i.a.w. the requirements for communications and IT support as described in this document for the classified information system architecture. The Contractor shall provide end user support for the CENTRIXS Communities of Interest Network enclaves (GCTF and CMFC) as well as U.S. Battlefield Information Collection and Exploitation System (USBICES). End user support consists of but is not limited to installation and configuration of desktop systems to include peripherals, responding to service requests, providing service center support, and coordinating actions with the back-end IT service provider.

C.5.5.2 STORAGE MANAGEMENT SUPPORT

The Contractor shall assist the Government in establishing the necessary physical and virtual storage to host and retain data for purposes such as content staging, continuity of operations or archival. The Contractor shall assist the Government in identifying and matching the capacity of the IT services and infrastructure to the current and future identified needs of the business. The Contractor shall assist the Government in establishing a framework that covers a range of component capacities and the design/deployment of capacity in order to meet expectations of data collection and analysis for infrastructure utilization and performance. The Contractor shall perform assessments as to whether there are potential problems and issues that must be addressed, and provide the results to the Government. The Contractor shall provide the following storage management support:

- Maintain and manage HOA-based storage devices, including analysis of capacity and execute generation of standard capacity reports for the designated Government manager of that storage device, system, or component.
- Ensure that cost-justifiable IT capacity always exists and is matched to the current and future identified needs of the business.
- Accommodate scalability requirements.
- Avoid incidents caused by lack of capacity.
- Operated and maintain the storage environment of critical IA logging data stored for forensic analysis i.a.w. AFRICOM guidance.

The Contractor shall consider the following elements for all Storage Capacity Planning:

- Reliability - the time for which a component can be expected to perform under specific conditions without failure.
- Scalability - the ability to expand network storage capacity, often utilizing an appliance to easily add storage and track storage growth to organization growth.
- Flexibility - the ability to add applications (e-mail, databases) to the networked storage; flexibility can be added by using a device that can handle application storage or share files.

C.5.5.3 CONTINUITY OF OPERATIONS (COOP), DISASTER RECOVERY (DR), AND BUSINESS CONTINUITY PLANNING SERVICES

The Contractor shall develop and document (for inclusion in overall COCOM plans) regional COOP, DR and business continuity plans consistent with existing/planned architecture and redundancy characteristics. The Contractor shall:

- Support, operate, and maintain COOP capabilities
- Develop, maintain, and annually update the regional DR Plan
- Provide input and assist the Government in developing system and network designs that enable business and network operations capable of surviving individual component failure.
- Provide input to the Government for making system degradation decisions in the event of a disaster or incident.
- Provide input to the Government After Action Reports (AARs) and lessons learned following exercises and recovery events.
- Support execution of emergency failover COOP requirements.
- Support annual exercise of the Disaster Recovery Plan (DRP).
- Activate the assigned components of the plan when required due to system failure, disaster event, or exercise.
- Assist in the implementation of continuity of operations activities.

C.5.5.4 CAMPUS AREA NETWORK (CAN) AND WIDE AREA NETWORK (WAN) ADMINISTRATION SERVICES

CAN and WAN Services include the installation, operation, and maintenance of the switching infrastructure that supports the delivery of IP-based voice, video, and data services on NIPR, SIPR and Coalition enclaves. The Contractor shall:

- Operate and maintain the CAN infrastructure including all supporting equipment (including but not limited to Layer 2 and Layer 3 switches, alarmed carrier devices, uninterruptible power supplies, inline network encryption, etc).

- Develop, maintain, and annually update the Master IP Routing Schema.
- Update design documentation to support all changes, new services, and technology refresh installations.
- Provide capacity and utilization monitoring of all CAN components.
- Notify the Government if the addition of a network device or service will exceed 75% of existing port capacity, transport infrastructure element (e.g., rack space), WAN access circuit capacity, WAN subscription capacity, inside cable plant, or outside cable plant utilization.
- Maintain Internet Protocol version 4 and version 6 (IPv4/IPv6) coexistence and interworking practices.
  - Operate and maintain dual stack IPv4/IPv6 network devices.
  - Develop, plan, and implement migration to a full IPv6 environment.
- Operate and maintain CAN and WAN interfaces for designated FOL sites within the CJOA.
- Comply with IA guidance prior to connecting any new device to the AFRICOM information systems.
- Comply with the DoD Ports, Protocols, and Services for configuration of assigned transport infrastructure.
- Maintain and update the technical and security architecture (e.g., IP unicast and multicast at the network layer and Ethernet at the physical layer) consistent with the Category Assignments List.
- Maintain and configure VLANs (e.g., provide single VLANs, multiple VLANs within a DMZ, and TLA) as necessary to support Access Control List requirements.
- Maintain and update SW and firmware required for CAN and WAN components.
- Conduct annual service continuity CAN and WAN site assessments, identify deficiencies, and provide future design and operations recommendations.
- Provide an analysis of major CAN and WAN single points of failure and recommend architectural modifications.
- Install and document site modifications to connect CAN to local DISN Service Delivery Point (SDP) i.a.w. site WAN circuit mapping.
- Maintain WAN routing in the Master IP Routing Schema.
- Install and test circuit and base extensions, including coordination with Base Communications Office (BCO), DISA, and Government Manager for end to end testing and activation of DISN circuits.
- Document WAN interface HW and SW to support Certification and Accreditation.
- Operate and maintain Multi-Protocol Label Switching and Quality of Service (QOS) where enabled.
- Install, configure, and manage NSA Type 1 Encryptors.
- Monitor network status and resolve connectivity issues associated with all supported enclaves (NIPR, SIPR and Coalition).
- Protect SECRET and below data in transit as specified in protection mechanisms required by DoDI 8500.2, Information Assurance (IA) Implementation.
- Comply with the SIPRNet Connection Approval Process security standards and the Defense IA Security Accreditation Working Group security requirements.

C.5.5.5 VOICE OVER INTERNET PROTOCOL (VoIP) AND VOICE OVER SECURE INTERNET PROTOCOL (VOSIP) SERVICES

VoIP/VoSIP Services enables voice communications over an IP network interfaced with the Public Switched Telephone Network (PSTN). This service provides the requisite HW and SW to permit the use of VoIP. IP phones provide end users with all the standard telephony features, including full voice mail capabilities and the option to customize ring tones and color display features. The CLDJ VoIP/VoSIP system supports communications via digital handsets, computer terminals, and conference speakerphones. DSN trunks, NSA approved Type-1 encryption devices, and DSN circuits will be GFP.

The Contractor shall:

- Operate and maintain assigned VoIP/VoSIP components in compliance with DoDI 8100.04, DoD Unified Capabilities (UC), relevant security requirements, and VoIP relevant STIGs in order to deliver assured services capabilities:
    - Media servers.
    - Application servers.
    - End user devices and handsets.
- Support engineering and design of VoIP/VoSIP services to include unlimited local connection minutes for basic telephone functionality.
- Support system HW and SW de-installation, move, re-installation, and change.
- Support engineering and design to provide access to toll free numbers.
- Support engineering and design to provide VoIP/VoSIP telephone system that interfaces between data services and the network on a fully converged voice and data LAN meeting DISA Unified Capabilities Requirements.
- Manage, maintain, operate, existing VoIP/VoSIP servers, switches, routers, and other equipment supporting VoIP networks.
- Maintain configuration of auxiliary voice VLANs.
- Maintain configuration, management, operations of network devices, PSTN interfaces, and fax modules supporting the voice system.
- Support VoIP/VoSIP moves, adds and changes (MACs) and complete other associated Service Desk network requests.
- Program, configure, and maintain the supporting network devices.
- Support VoIP services that provide Layer 3 switching capability as well as updated TACLANE configurations in support of DISA Voice over Secure Internet Protocol (VoSIP).
- Program, configure, and maintain VoIP service with capability to support Extension Mobility, Unified Messaging, and Emergency Responder.
- Program, configure, and maintain VoIP service that supports Call Center operations in a Service Desk environment.

C.5.5.6 RESIDENTIAL NETWORK CONNECTIVITY

The Contractor shall provide Systems Analysis, Systems Engineering, System Administration, Information Assurance, connectivity, and end-user support services for communications and IT for designated residential network access capability. The Contractor shall follow the approved CLDJ process and procedures for the identification, installation and support of all communications and IT capabilities in residences.

C.5.5.7 NON-PERMANENT REMOTE CONNECTIVITY AND MOBILE COMMUNICATIONS

The Contractor shall provide Systems Analysis, System Engineering, Systems Security and System Administration services to remote HOA users in support of designated AFRICOM information systems to include the following:

- Operate, maintain, and manage the regional components (e.g., Secure Sockets Layer Virtual Private Network client, certificate integration, and enterprise authentication) to give end users secure access to both the NIPRNet and SIPRNet from remote locations via commercially available wired and wireless broadband internet access.

- Operate and maintain the VPN infrastructure resident at the TLA that supports end to end encryption for both clients and remote sites enabling end users to establish a secure, encrypted tunnel to AFRICOM network resources.
- Operate and maintain classified remote access services to the AFRICOM classified enclave with approved remote computing devices via approved GFP secure dial up capability and certified Type-1 cryptographic devices.
- Provide IT support to deployed and TDY regional users who have accounts on existing supported networks and systems
- Provide a laptop library system to provide for the short-term IT needs of mobile or deployed users
- Provide support for encrypted disk security configurations for mobile laptops and remote workstations.
- Configure and maintain access control lists for remote access to networks
- Provide and maintain Government approved boundary VPN HW and SW
- Operate and maintain VPN connections between all points of presence for the unclassified network.

C.5.5.8 HOA SUPPORT WIDE AREA NETWORK (HSWAN)

HSWAN is a hosted service with remote users being supported by the J6 staff and their vendor for both the transport and system at the remote location. The Contractor shall provide:

- Entry point(s) into the AFRICOM information system enclaves as required
- Access to the AFRICOM SDC for use at the remote sites
- Access to patches and updates information for IA Compliancy
- C&A guidance and review of their interconnection documentation

C.5.5.9 VISUAL INFORMATION AND PRESENTATION SERVICES SUPPORT

VTC Services are comprised of the HW, SW, network, and scheduling services necessary to deliver real time video and audio communications between end users at two or more locations. VTC Services include: 1) cameras; 2) coder-decoder (CODECs); 3) monitors; 4) onscreen menus; 5) dynamic speaker technology; 6) far-end camera control; 7) collaborative tools; 8) VTC scheduling set-up and operations; 9) IP infrastructure; 10) multi-session; 11) Multi-point Control Unit (MCU) bridging service; and, 12) remote diagnostics. The VTC Services provide VTC connectivity throughout the AFRICOM network and with external participants via high bandwidth communications, point-to-point, and point-to multi-point switching.

The Contractor shall provide support for AFRICOM Visual Information and presentation service systems. These systems include, but are not necessarily limited to, the following:

- Defense Information Systems Network (DISN) Video Services (DVS) Video Teleconferencing (VTC) Facilities
- Classified, IP-based VTC Systems;
- Collaborative Tools requiring video capabilities;
- Portable or other mobile VTC capabilities
- Secure desktop video phone device (Tandberg 1000s or similar)

The Contractor shall:

- Perform VTC scheduling and manage Command assets used for scheduling and bridging VTC events. The Contractor shall coordinate reservation and scheduling of VTC services with outside agencies when required.
- Perform VTC set up and operations, multi-session bridging, and other related administrative tasks in order to enable VTC connectivity both with internal and external participants. The scope of this support includes but is not limited to assisting end users in operating equipment and in establishing, maintaining and troubleshooting VTC connectivity throughout the duration of the video-conferencing session. The Contractor shall support both point-to-point and simultaneous point-to-multi-point connections.
- Provide remedial and preventative maintenance, hardware integration of comparable components, provide user and operator level training, management of user accounts, and develop and maintain system documentation for systems.
- Perform remote diagnostics in order to maintain, restore or otherwise establish connectivity.
- Maintain a record of all VTC operations and provide a VTC Usage Report to the Government.
- Provide when direct Presentation services and support for critical users in the areas of broadcast communications, to include singular events and/or collaborative on-line events.

C.5.5.10 NETWORK CRYPTOGRAPHIC SUPPORT SERVICES

Network Cryptographic Support Service is the use of encryption technology to cryptographically separate information at different levels of classification that permits that information to be communicated via a common infrastructure and even “tunneled” across a non-secure public Internet.
Procurement of most items associated with cryptographic equipment remains an inherently governmental responsibility.

Note: In HOA, the crypto footprint currently includes Army assets(WAN) and Navy assets (CAN).

The Contractor shall manage and safeguard Government provided encryption products and keying materials and perform cryptograhic equipment support services i.a.w.:

- <u>Army assets</u>: COMSEC Material Direct Support Activity (CMDSA) user account guidelines and training.
- <u>Navy assets</u>: EKMS-1 Series, Communication Material System Policy and Procedures for Navy Electronic Key Management System (EKMS).

The Contractor shall provide cryptographic equipment support to include:

- Use, safeguard, operate, and maintain cryptographic material i.a.w. appropriate Government policy and processes.
- Operate and maintain Government provided Type 1 encryption when supporting classified and coalition networks.
- Maintain accountability of cryptographic keying material i.a.w. governing regulations.
- Install, configure, maintain, and re-key encryption devices as necessary to support continuous operations.

C.5.5.11 SYSTEM ENGINEERING SUPPORT

HOA On-site engineering efforts performed by the Contractor shall be limited to integrating new hardware and software into their existing baselines. All other engineering efforts are typically performed either by other on-site associate contractors in the HOA region or by the Contractor’s engineering team located with AFRICOM on Kelly Barracks.

C.5.5.11.1 SYSTEM INTEGRATION

As services and technologies evolve, new software and hardware will need to be incorporated into the existing baseline as determined by the applicable Government agent. In addition new security measures will be developed, issued, and require implementation, and therefore will need to be integrated into existing baselines. The Contractor's effort shall include:

- Test and evaluate commercial-off-the-shelf applications, Government-off-the-shelf applications and hardware for integration into the C4 networks
- Ensure compatibility with current baseline resolving conflicts as they arise
- Apply appropriate security measures (STIGs, IAVMs, Tasking Order Compliance…etc) to lock down the application/hardware
- Develop deployment procedures (i.e. package software, installation instructions…etc)
- Have Information Assurance review and sign-off acceptability prior to deployment
- Test and evaluate IA directed patches for compatibility with the current baseline and resolve any conflicts prior to deployment

C.5.5.12 INFORMATION ASSURANCE SERVICES

The Contractor shall assist AFRICOM with the implementation of IA strategies for all AFRICOM accredited networks at HOA, consistent with DoD and National Security Agency (NSA) guidance. The Contractor shall provide services and support to ensure the confidentially, integrity and availability of AFRICOM accredited C4 networks at HOA. AFRICOM requires all C4 networks be protected from network attacks, unauthorized access, service interruption and unauthorized disclosure or modification of information that is processed on them. The Contractor will research, develop and implement a holistic risk management strategy for C4 networks to enable the execution of AFRICOM and HOA operations.

The networks at HOA are accredited as extensions of the AFRICOM networks therefore the DAA/AO is responsible for all HOA Information Assurance activities. The IA function in HOA (while geographically separated) will act as an extension of AFRICOM IA following their lead, guidance, and policies.

Information Assurance is highly regulatory in nature and strict adherence to the DOD directives listed in the Attachment A - Specific Governing Documents as well as AFRICOM's instruction, policies, and procedures is required. Several tasks described below referencing "when directed" means the Contractor shall take direction from AFRICOM's Designated Approval Authority (DAA)/ Authorizing Official (AO), AFRICOM's Information Assurance Manager (IAM), and others as designated in writing by the DAA/AO/IAM.

C.5.5.12.1 INFORMATION ASSURANCE PROGRAM MANAGEMENT

The Contractor shall provide the following support and services:

- Implement and manage the AFRICOM network security policy.
- Manage and maintain the Certification and Accreditation (C&A) program for communications and information systems under the purview of HQ AFRICOM.
- Prepare for, assist with, and monitor IA assessments (network readiness assessments, DISA Security Readiness Reviews (SRR), Command Cyber Readiness Inspections, NSA Red and Blue Team assessments, vulnerability scans, certification and accreditation reviews). Develop and/or implement corrective courses of action for findings identified during these assessments. Resolve open security vulnerabilities in a timely manner focusing on most critical vulnerabilities first.

- Ensure all internal (CITS Contractor) personnel granted elevated privileges or performing IA functions on AFRICOM systems/networks are trained and certified i.a.w. the DoD Manual 8570.01M, Information Assurance Workforce Improvement Program.
- Maximize use of external organizational reciprocity agreements in support of DIACAP or RMF compliancy.
- Integrate information assurance and security principles in the Change Management process in the design and development phase.
- Develop technical standards (SOP/TTPs, technical implementation instructions, or other required documentation) for security devices, security operations and other operations as required for Government approval. Ensure all technical standards are updated, maintained, and centrally located for distribution as needed.

C.5.5.12.2 CERTIFICATION AND ACCREDITATION (C&A)

The Contractor shall provide the following support and services:

- Manage and maintain the Certification and Accreditation (C&A) program for communications and information systems under the purview of HOA
- Prepare and maintain DIACAP or RMP artifacts/packages (e.g. Configuration Management Plan, Vulnerability Management Plan, System Plan of Action and Milestones, IT Continuity Plan, Security Design Management Process, Security Requirements Traceability Matrix…etc.) i.a.w. applicable Government directives and policies
- Develop and maintain C&A documentations including Program of Record (POR) and Program Managed Systems for SIPRNet and NIPRNet connection approval processes
- Validate accreditation worthiness by performing vulnerability scans and DISA STIG checks
- Prepare and maintain Risk Management Framework artifacts/packages when required or directed
- Maintain a copy of all network documentation to include DIACAP or RMF packages, network diagrams, IP ranges, COOP and disaster recovery plans, and the number of systems by type
- Ensure C&A documentation is populated and maintained in the appropriate SIPRNET or NIPRNET Enterprise Mission Assurance Support System (eMASS)
- Ensure systems are established and maintained in accordance applicable C&A directives to include being compliant with the IA Controls and/or RMF Controls assigned by the specified MAC levels
- Serve as Information Assurance point of contact for new, replacement, trial, or test equipment or software being brought into the purview of the AFRICOM HOA accreditation boundary. Ensure the sponsor and/or action officer provide necessary accreditation documentation before fielding, demonstrating, or testing the product
- Evaluate the security risks and provide recommendations on requests to add software and hardware to the Approved Product List
- Integrate with the Change Management process ensuring:
    - Systems have approval to connect or operate
    - The required change has met all security requirements
    - All C&A documentation impacted by the change is updated
- Perform on-site IA C&A assessments on AFRICOM HOA networks and systems at the direction of the Government. (Note: DoD directives require that approximately 33% of the packages must be assessed each year)
- Assist, develop, and recommend corrective courses of action for findings identified during network readiness assessments, vulnerability scans and certification and accreditation reviews.

For findings directly associated with C&A documentation and processes resolve open security vulnerabilities, focusing on the most critical vulnerabilities first.

- Maintain Information Assurance tools/systems required to support C&A functions when required or directed
- Review, provide input, and (with Government) respond to internal and external taskings

C.5.5.12.3 COMPUTER NETWORK DEFENSE (CND)

The Contractor shall provide the following support and services:

- Take appropriate measures as directed by the CNDSP to respond to known and possible network attacks in accordance with applicable DoD policies, directives and instructions
- Develop and recommend internal policies and procedures for handling network related incidents and protecting networks. Archive and audit security event logs in accordance with DoD policy, and if applicable NATO security policy.
- Report, mitigate and/or resolve all classified security incidents (e.g. data spills, unauthorized disclosures of classified information) that impact networks within time constraints identified by applicable directive
- Report, mitigate and/or resolve all network anomalies (e.g. unauthorized network access, etc.) that occur on assigned networks ICW the CNDSP Tier III Service Provider
- Develop and manage incident response actions (e.g. Tactics, Techniques and Procedures) ICW the CNDSP Tier III Provider and AFRICOM J62
- Report incidents to the CNDSP Tier III Provider, AFRICOM J62, AFRICOM ACCC, and the DAA/AO.
- Support incident reporting activities in accordance with DoD, AFRICOM and CNDSP Tier III policies and directives. Collaborate and interface with external organizations/agencies on security related issues and investigations.
- Maintain assigned Information Assurance tools systems (i.e.: firewalls, encryption tools, Intrusion Detection Systems, Intrusion Prevention Systems, Vulnerability Scanning systems, Security Event and Information Management system, Content Filtering, Correlation Systems, Malware protection systems, application and device control systems…etc) residing on AFRICOM HOA networks. Ensure all changes to Information Assurance network security devices (e.g. firewalls, IDSs, IPSs, sensors, etc.) are submitted to and approved by the CAB/CCB.
- Support and provide the necessary information (e.g. firewall logs, system logs, storage media, etc.) to the Stuttgart Regional Network Analysis Lab (SRNAL) and other government designated organizations in the performance of CNDSP activities and forensic analysis services for AFRICOM, DISA-AF, 5SC and partner/affiliated organizations.

C.5.5.12.4 INFORMATION ASSURANCE COMPLIANCY

The Contractor shall provide the following support and services:

- Support and ensure AFRICOM HOA networks are compliant with the DoD Information Assurance Vulnerability Management (IAVM) Program
- Evaluate and implement all applicable Information Assurance Vulnerabilities, Bulletins and Technical Advisories i.a.w. CYBERCOM directives.
- Report IAVM compliancy; track CYBERCOM Command Tasking Orders (CTOs), FRAGOs, INFOCON; Coordinated Alert Messages (CAMs), and other directives for AFRICOM network assets hosted in the HOA region through the Vulnerability Management System (VMS).
- Ensure weekly compliancy reports are compiled and sent to the AFRICOM. Perform analysis, implement, and report the compliancy of CYBERCOM tasking orders.

- Populate assets and maintain security vulnerability compliancy through the VMS for AFRICOM HOA network assets including POR systems.
- Perform vulnerability scans/checks on all AFRICOM HOA network assets including POR systems and ensure periodic audits are done using the Gold Disk, Retina/Assured Compliance Assessment Solution (ACAS) or other DoD approved vulnerability scan tools. Evaluate and ensure security threats are mitigated, remediated or waived i.a.w. accepted time constraints.
- Comply with DoD ports and protocol management program. Track and document approved "opened" ports and protocols inbound and outbound.
- Manage and monitor the IA posture/compliancy of Secret and Below Interoperability (SABI)/ CDS devices.
- Conduct periodic internal audits to ensure compliance of the IA Workforce Improvement Program; resolve discrepancies if found.
- Manage the DoD 8570.01M program for the staff at CLDJ
- Document and maintain an approved software and hardware baseline for all Information Systems under the purview of AFRICOM within the HOA region. This includes, but is not limited to routers, switches, servers, workstations, printers, and digital senders, etc.

C.5.5.13 LOGISTICS MANAGEMENT

C.5.5.13.1 CONFIGURATION MANAGEMENT

The Contractor shall follow 5th Signal Command's Configuration Management Plan, processes, and procedures providing configuration management of the AFRICOM C4 networks and systems, inclusive of the networks and information systems that extend to the HOA region. The Contractor is a participant and not the process owner.

The Contractor shall assist 5SC and AFRICOM with maintaining a disciplined configuration management program that encompasses documented change control procedures and practices for hardware and software on supported networks/systems, to include coalition.

It is expected that the within the construct of 5SC's overarching Configuration Management Plan, that the Contractor employ disciplined practices in supporting 5SC CAB and AFRCIOM CMB activities; documentation processes; and in performing timely, accurate update and maintenance of configuration data for supported communications and IT software and hardware.

C.5.5.13.2 ASSET MANAGEMENT

The Contractor shall maintain AFRICOM's and HOA's inventory of spare equipment to include Property Book/Hand Receipt items and other IT supplies such as operating stock and/or bench stock. The Contractor shall establish, follow and manage all communications and IT assets throughout all aspects and phases of the life-cycle. The Contractor shall propose processes, tools and procedures in order to accomplish this. The Government shall approve the formal Asset Management process, procedures and tools to be used. The Contractor shall administer this program and account for all communications and IT assets for AFRICOM and CJTF-HOA in support of the appropriate Government responsible agent. Life cycle management and disposal of assets ensures that AFRICOM and CJTF-HOA assets are maintained and updated until criteria for retirement are met and the assets are returned to storage in preparation for disposal. Assets that have reached end-of-life will be disposed of as required. Asset records and databases must be updated with new information and a change in asset status.

The Contractor shall:

- Maintain accountability of HW and store significant information about each asset, such as:
  - *i.* Manufacturer, make, model, serial number.
  - *ii.* Purchase orders including approving authority.
  - *iii.* accurate and timely warranty data information
  - *iv.* Vendor information.
  - *v.* Financial information.
  - *vi.* Any related contracts or documentation.
- Perform Property Book/Hand Receipt Holder duties, inventory management, and accountability functions for all network and end user data, voice, VTC and wireless equipment under their control
- Perform receiving, storage, staging, and distribution functions for data, voice, VTC and wireless equipment (network and end-user)
- Identify and report to the government equipment that is either lost or damaged beyond economical repair
- Identify and report to the government any excess or end of life equipment
- At the end of service life, demilitarize and dispose of HW and SW at cleared Government facilities i.a.w. applicable DOD guidance
- Ensure resources (stock) that the Government already owns are employed before purchasing new additional items
- Recommend candidate equipment to the government for lifecycle replacement semi-annually or upon Government request
- As directed by the responsible Government agent turn-in excess or end of life equipment on the Contractor's Property Book
- Identify and implement best practices and technologies for an effective asset management program
- Track and account for storage media (e.g. hard drives, backup tapes) that process and store NATO SECRET information in accordance C-M (2002)49, "NATO Security Policy". AFRICOM SIPRNet is classified up to U.S. SECRET and NATO SECRET

C.5.5.13.3 LICENSE AND SUBSCRIPTION MANAGEMENT SERVICES

The Contractor shall assist the Government in maintaining the license database. For HOA, all software subscription services, licenses, maintenance, software assurance support, etc is performed i.a.w. AFRICOM processes. Refer to AFRICOM PWS section C.5.3.6.2, SUBSCRIPTION MANAGEMENT SERVICES.

Note: Stored information typically includes:

- *i.* Software information including name, version, release.
- *ii.* Purchase orders including approving authority.
- *iii.* Vendor information.
- *iv.* License type.
- *v.* License allocation.
- *vi.* Financial information.
- *vii.* Related contracts or documentation.

C.5.5.13.4 STANDARD DESKTOP CONFIGURATION MANAGEMENT

The Contractor shall use the 5th Signal Command approved and managed Standard Desktop Configuration in their maintenance actions. The Standard Desktop Configuration (SDC) will be managed by the 5SC Change Advisory Boards (CAB) with representation from AFRICOM.

The Standard Desktop Configuration is comprised of the desktop Operating System (OS), core applications (e.g., Microsoft Office Suite, Java, Adobe Reader, and anti-virus), as well as HW specific configuration items and the associated configuration characteristics for a specific workstation platform. Changes to the SDC occur when 1) specific SDC components are updated; 2) new components are added to the SDC; 3) security patches are applied to the components in the SDC; or, 4) existing SDC components are retired and removed from the SDC.

C.5.6 MULTI-NATIONAL INFORMATION SHARING (MNIS) SYSTEMS

The Contractor shall provide EUCOM the full range of network O&M support for their MNIS networks – SEAGULL and CENTRIXS albeit on a limited scale. Although scaled to meet the requirement, The Contractor shall mirror those services already describe in this paragraph (C.5) – network administration, system administration, system monitoring, planning and engineering, information assurance, GCCS system administration, customer support to include remote sites, VOIP services and configuration management. GCCS system administration is not required for CENTRIXS however shall be provided for USBICES and SEAGULL.

C.5.7 THEATER SECURITY COOPERATION MANAGEMENT INFORMATION SYSTEM (TSCMIS)

The Contractor shall function as the database administrator (DBA) and Systems (.Net) Programmer for TSCMIS and its corresponding EUCOM/AFRICOM-specific related databases while providing the customer with technical guidance for satisfying functional requirements and overall planning. These duties include recommending improvement, importing and exporting data, upgrading the database to new versions of SQL Server, responsibility for the Extensible Markup Language (XML) schema, and responsibility to act as the database liaison with the DB Program of Record office for all enhancements. DBA duties include data imports and exports, and troubleshooting database connection issues and building maintenance schemes. Systems Programmer duties shall include ensuring the ability of both COCOMs to publish and pull TSC information from the TSCMIS Enterprise Messaging Bus or other proscribed means/methods of TSC information transfer.

The Contactor shall provide Operation Management subject matter expertise, implementation of authorized changes and maintenance of TSCMIS that refine and enhance the functionality of TSCMIS while maintaining compliance with the TSCMIS baseline system. In doing this, the Contractor shall conform to the priorities and timelines established by the functional requirements of user communities as prioritized by members of COCOM IT staff. The Contractor shall ensure compliance with the TSCMIS Project Management Office, Configuration Control Board for changes against the baseline system. The Contractor shall also facilitate the operation of the system remotely to other organizations as determined by the functional user (J5/8) and authorized by ECJ6 staff.

The Contractor shall further develop, maintain and integrate the EUCOM Concept and Funding Request (CFR) Database ensuring current TSCMIS and future G-TSCMIS compliant module is operative allowing for its potential integration into the G-TSCMIS concept. To this end the Contractor will work all assigned BugNet user issues through resolution and adaptation.

The Contractor shall further develop, maintain and sustain current EUCOM/AFRICOM specific systems (Dashboard, SAS Tool and TREX Integration/Functionality) that provide a comprehensive picture of whole-of-government Security Cooperation's activities to assist decision makers, planners and other users with the ability to view, manage assess and report security cooperation activities and events. TSCMIS data is currently used to feed current and future EUCOM/AFRICOM Commander Decision Boards, SAS Tool and TREX (Theater Security Cooperation Records Exchange) modules. The requirement for these databases to exist and remain operational at EUCOM/AFRICOM is valid until G-TSCMIS can fully assume these functions for both COCOMs.

C.5.8 SPECIAL OPERATIONS COMMAND AFRICA (SOCAFRICA)

Special Operations Command Africa (SOCAFRICA) requires services as described in paragraph C.5.10 for enterprise networks and services used within in their Area of Responsibility. The Contractor shall provide operational systems development services to support the rapid deployment of new system, and the improvement to existing systems, with a primary focus on meeting the operational and technical requirements of all programs/projects. The scope is limited to providing in-garrison support; down-range support and deployment of contractors is outside the scope of this requirement with the exception of short duration TDY to support requirements gathering. The service shall be provided on a level of effort basis rather than performance basis. The Government request the Contractor provide personnel:

Senior System Engineer - The Contractor shall provide services and support to plan and engineer adequate communications system solutions to meet SOCAfrica mission requirements. Engineering capability should be sufficient to engineer and plan communication solutions for both garrison (enterprise) and deployed environments. This includes in depth technical understanding of, and the ability to provide communications solutions that utilize, the following: (list is not exhaustive)

- Antenna, Aerial, Dish & Radom
- Radio and Transceiver (including data, i.e. HPW, PDA184)
- Communications Vaults & Outbuildings
- Conveyances
- Telecommunications (TELECOM)
- Satellite Communications (SATCOM)
- Airborne Satellite Systems (KuSS technologies, antennas, modems, etc)
- ISR distribution technologies (UVDS, GBS, etc) and ISR Aircraft platforms
- IP networks (routing, switching, VPNs, etc).
- Wireless networking (IEEE 802.11, 802.15, 802.20)
- Cellular-based communications (2G/3G/4G; Voice and Data)

Senior IT Project Manager – In addition to project management functions the Contractor shall conduct mission and operational analysis to provide a traceable operational foundation for systems requirements and program development. This operational analysis also provides the basis for identifying specific operational intent and understanding for overall entity relationships and information flows at strategic, operational, and tactical levels; includes mission and operational analysis, organization analysis, and process/workflow analysis and definition.

Senior Network/Systems Engineer – Provides systems/network/LAN/WAN expertise and support to monitor, manage and provide resolution to systems supporting SOCAFRICA and its supporting units.

Define maintenance planning requirements, and conduct periodic maintenance and monitoring of critical C4ISR platforms required to support SOCAFRICA's mission. The Contractor will provide system support expertise in the following areas

- Platforms: Directory Services; PKI, Client and Server Operating Systems
- Messaging: Exchange, LYNC, Blackberry, SMEPED, Mobile Devices
- Storage: SAN, SQL, Backup, Virtualization
- Management/Monitoring: SCOM, SCCM, SPECTRUM, Imaging, Updates, Deployment, Circuit Status, SolarWinds
- Portal: IIS/TMT/SharePoint/IE
- Situational Awareness: COP, GCCS-J
- Networking: Routing/Switching/Firewalls/VOIP
- SATCOM: Tactical Satellite, All relevant bands (Ka, Ku, KuSS, C, X)

GCCS System Administrator – duties as described in paragraph C.5.3.3

C.5.9 SECTION 508 COMPLIANCE

Unless the Government invokes an exemption, all EIT products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 CFR 1194. The Contractor shall identify all EIT products and services proposed, identify the technical standards applicable to all products and services proposed and state the degree of compliance with the applicable standards. Additionally, the Contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The Contractor must ensure that the list is easily accessible by typical users beginning at time of award.

The Contractor must ensure that all EIT products and services proposed that are less than fully compliant, are offered pursuant to extensive market research, which ensures that they are the most compliant products available to satisfy the solicitation's requirements.

If any such EIT product or service proposed is not fully compliant with all of the standards, the Contractor shall specify each specific standard that is not met; provide a detailed description as to how the EIT product or service does not comply with the identified standard(s); and shall also indicate the degree of compliance.

C.5.10 TECHNICAL REFRESH/INTEGRATION SERVICES

The Contractor shall develop, maintain and submit a Communications and IT Refresh/Integration Milestone Plan, with Quarterly Updates, for communications and IT refresh and integration support. The Technical Refreshment/Integration & Milestone Plan shall include the anticipated costs and supporting build-up detailing projected costs for the proposed refresh/integration work.

Consistent with the Government approved Technical Refreshment/Integration & Milestone Plan, the Contractor shall provide communications and IT refresh/integration services. The Contractor shall identify, document and provide processes and methodologies necessary to retrofit and integrate communications and IT hardware, software and devices to the Government. The Government shall be the approval authority for the conduct of technical refresh/integration activities. Upon receipt of

Government approval, the Contractor shall acquire equipment, hardware, and software deemed necessary to meet or exceed current and/or emerging requirements for communications and IT.

Technical refresh shall incorporate methods for economically delivering commercially available products to the Government. The Contractor shall provide for economies of scale and ensure recommended/chosen technologies and equipment/capabilities perform to the current and anticipated technological environments.

C.5.11 PURCHASING

The Contractor shall purchase communications and IT assets in accordance with Alliant Contract H.18. All purchases shall be approved by the GSA COR, consistent with DoD and Army Acquisition Policies, e.g., the use of the Computer Hardware, Enterprise Software Solution (CHESS) contract vehicles for tool purchases. In general, the Tools CLIN is anticipated for the purchase of communications and IT assets to update, maintain, establish or enable sustained communications and computing capabilities for the technical environments that are covered under the scope of this Task Order. Purchases are expected to include hardware and software including, but are not limited to servers, network gear inclusive of switches, routers, NICs, hubs; laptops, desktops, handheld devices, storage devices and media; projectors, video telecom equipment, components, accessories, audio gear, displays, & related peripherals; VPN gear; scanners & tag readers; miscellaneous peripherals, component parts & supplies, such as cables, couplers, connection kits; licensing and maintenance of operating system and application software products, security software and information assurance products; and related subscription-style technical and consultative-type services to enable productive deployment and efficient use of such hardware/software.

The Contractor shall ensure that all communications and IT hardware provided has the most cost-effective warranty available from the vendor. In most cases, warranty coverage should be for parts only versus on-site warranty coverage. The Contractor shall use its Government approved purchasing procedures to procure requisite items under the Tools CLINs.. Proposed purchases shall be integral and necessary to the overall Task Order performance, and approved by the COR in writing prior to execution (Email will suffice).

The Contractor shall categorize all procurements as either: (1) in support of an emergency (Mission Critical), (2) contingency operations (Urgent), or (3) routine (daily operation). The Contractor shall notify (and, if necessary, request clarification from) the COR for all purchases requiring Mission Critical ordering.

The Contractor shall maintain property accountability records and sub-hand receipts of all contractor-purchased equipment or Government-provided equipment used in its daily communications and network operations. Copies of all purchasing invoices for all property book items procured under this Task Order shall be submitted to the appropriate command Resource Management (RM) and Supply/Property Book Office.

C.5.12 ASSOCIATE CONTRACTOR CONSIDERATIONS

There are functions within the scope of this Task Order where the Contractor must cooperate, share information, or otherwise jointly collaborate in the accomplishment of the government's requirements with other associate contractors working on separate government contracts. Where such contractor-to-contractor interfaces arise, the contractor is expected to establish professional, collaborative relationships with associate contractors to ensure the greatest degree of cooperation in providing technical solutions and services to successfully support mission needs within required time and cost constraints.

C.5.13 PROGRAM MANAGEMENT

The Contractor shall provide program management support under this Task Order. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors/teaming partners, to satisfy the requirements identified in this Performance Work Statement (PWS). The Contractor shall identify a Program Manager (PM) by name, who shall provide management, direction, administration, quality assurance, and leadership of the execution of this Task Order. The Contractor shall identify Contractor Site Leads and Technical Leads by name, who shall, in concert with the Contractor's PM, provide day-to-day operational level leadership and technical guidance to contractor personnel performing work under this Task Order.

[Note: See Section H.4 for additional information about the PM and Site Leads.]

C.5.13.1 PROGRAM MANAGEMENT PLAN (PMP)

The Contractor shall document and maintain an up-to-date Program Management Plan (PMP). The Contractor shall submit the PMP within 30 calendar days of the effective date of the Task Order. The PMP shall describe the proposed management approach. The PMP shall detail Standard Operating Procedures (SOPs) for all tasks. The PMP shall include milestones, tasks, and subtasks required in this Task Order. The PMP shall provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations. The PMP shall include the Contractor's Quality Control Plan (QCP), Risk Management Plan (RMP) as well as communications and change management processes to be followed. The PMP shall include, but not be limited to, Process Management and Control (to include monitoring mechanisms, i.e. Program Metrics, and Response to Customer Needs), Personnel Management (to include coverage and organizational structure), Financial Management (to include cost containment and cost forecasting), and Technical Effectiveness (to include routine Operation and Maintenance, and implementation and integration of new hardware and software, and technical refresh procedures).

The Contractor shall ensure the PMP is accessible electronically and shall be prepared to brief PMP content to the Government on 24 hours notice.

The PMP shall include establishment of task support in relation to incrementally provided funding i.a.w. customer established task priorities. The PMP shall document prioritization of support to be performed, level of service, and estimated staffing. The Contractor PM will review the PMP with the GSA COR and customer Client Representative (CR) on a monthly basis.

C.5.13.2 PROJECT ENGINEERING PLAN

The Contractor shall provide a monthly Project Engineering Plan (PEP) for managing backlog of project requests. The monthly Project Engineering Plan shall include status of short term and long term projects.

C.5.13.3 CONTRACT ACTIVITY AND STATUS MEETINGS

The Contractor Program Manager shall convene a monthly Contract Activity and Status Meeting with the TPOCs, COR, and other government stakeholders. The scheduling for the Contract Activity and

Status Meeting will be at a date and time mutually agreeable to the Contractor and the TPOCs/COR. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activity and status report, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The Contractor shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five calendar days following the meeting.

The Contractor shall provide the Government real-time access to metrics on communications and information technology support, to include actual statistics, trend analysis and performance measurements and assessments.

C.5.13.4 MONTHLY STATUS REPORT (MSR)

The Contractor shall develop and provide a MSR using common office productivity suite applications, by the 15th of each month via electronic mail to the Client Representative (CR) and the COR. Information included in the MSR shall be segregated in accordance with a Government approved format. The MSR shall include the following:

- Activities during reporting period, by task (Include: On-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- Personnel gains, losses and status (security clearance, TESA, etc.).
- Government actions required.
- Schedule (Shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Summary of Ad-hoc Technical Reports provided.
- Summary of trips taken, conferences attended, etc. Attach trip reports to the MSR for reporting period.
- Accumulated invoiced cost for each CLIN up to the previous month.
- Projected cost of each CLIN for the current month and forecasts through the end of the current performance period.
- Comparison data / monthly performance reports.

C.5.13.5 PROGRAM METRICS

The Contractor shall provide the Government with written Monthly Metrics which:

- Provide quantitative measurements which capture and evaluate communications and information technology support, identify trends, and measure performance.
- Serve as a measure of contractor effectiveness

The Contractor shall work with the Government to identify and incorporate specific measures to include: establishing the targets and acceptable quality levels for specific measures; methods of calculation and manner of collection; and the format for reporting. It is expected that program metrics will evolve from time-to-time as program needs change and will include performance standards cited in this PWS and other metrics applicable to the scope of services covered under this Task Order.

Note: Reference PWS Attachment J for historical information and benchmark metric data from the predecessor CITS Task Order.

C.5.13.6 TRIP REPORTS

The Government will identify the need for a Trip Report (if required) when the request for travel is submitted to the COR. The Contractor shall keep a summary of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, duration of trip, and POC at travel location.

C.5.13.7 DELIVERABLES

The following schedule of milestones and deliverable submission dates will be used by the COR to monitor timely progress under this Task Order.

The following abbreviations are used in this schedule:

- N/A: Not Applicable
- i.a.w.: In accordance with
- NLT: No later than
- TOA: Task Order Award
- All references to days imply workdays, unless otherwise noted

DELIVERABLES.	DUE DATE / PLANNED COMPLETION DATE
Network Documentation	i.a.w. PMP
Maintenance Management Plan	i.a.w. PMP
Supported Equipment List	i.a.w. PMP
Maintenance Actions Summary Report	i.a.w. PMP
On-Call Rosters	i.a.w. PMP
Access Control Lists	i.a.w. PMP
Backup and Recovery Plan	i.a.w. PMP
COOP Exercise Reports	Annual
COOP Exercise Plan	30 calendar days prior to the anticipated start date of the exercise
VTC Usage Report	i.a.w. PMP
Voice Over IP (VOIP) Performance Metrics Report	i.a.w. PMP
Certification and Accreditation Documentation	i.a.w. PMP
Security Event Logs	i.a.w. PMP
Information Assurance SOP/TTPs	i.a.w. PMP
IA Compliancy Reports	Weekly, Every Wednesday
Plan of Action and Milestones (POA&M)	i.a.w. PMP
Engineering Assessments	i.a.w. PMP
System Documentation	i.a.w. PMP
Preliminary Studies	i.a.w. PMP
Strategic Planning Studies	i.a.w. PMP
Estimates and Schedules	i.a.w. PMP

DELIVERABLES.	DUE DATE / PLANNED COMPLETION DATE
Technical Studies	i.a.w. PMP
Draft Technical Policy	i.a.w. PMP
Network Architecture Plan	i.a.w. PMP
C4 Network Systems Documentation	i.a.w. PMP
C4 Systems Architecture Documentation • Draft C4 Systems Architecture Technical Product • Final C4 Systems Architecture Technical Product	i.a.w. PMP, Quarterly Updates Final Due 10 workdays after Government comment
C4 System Tests, Assessments, and Architecture Reports	i.a.w. PMP
Technical Implementation Instructions	i.a.w. PMP
Migration/Transition Planning Documentation	i.a.w. PMP
AFRICOM Engineering documentation: • Project Charter • Implementation Plan • Engineering Design Plan • Requirements Baseline Document • Project CONOPS	i.a.w. PMP
EUCOM Engineering documentation: • Requirements Document • Engineering Reviews • Implementation Plan • Test Plan • Test Results • O&M Turnover Documentation	i.a.w. PMP
• SME Support Activity Report • Audit report	i.a.w. PMP
Network Configuration Documentation	i.a.w. PMP
Configuration Control Board (CCB) Minutes	i.a.w. PMP
Property Accountability Records	i.a.w. PMP
Sub-Hand Receipts	i.a.w. PMP
Purchasing Invoices	i.a.w. PMP
Classified Data, Equipment and Devices Inventory	i.a.w. PMP
Communications & IT Refresh/Integration Milestone Plan	Quarterly Updates

DELIVERABLES.	DUE DATE / PLANNED COMPLETION DATE
Program Management Plan (PMP, inclusive of: • Quality Control Plan • Risk Management Plan • Communications and Change Management processes	Draft within 10 calendar days following the Kickoff Meeting Final within 10 workdays after Government comment; Updates, as required during performance
PMP Briefs	On 24 hours notice
Project Engineering Plan	Monthly
Contract Activity and Status Meetings Minutes	Within 5 calendar days following the monthly meeting
Monthly Status Report (MSR)	By the 15th of each month
Metrics Report	Monthly to coincide with submission of Monthly Status Report
Trip Reports	i.a.w. PMP
Technical Expert Status Accreditation (TESA) Documentation	i.a.w. PMP
Contractor Manpower Report	By October 31 of each calendar year
Kick-Off Meeting	Upon Task Order Award, as scheduled by the GSA CO or designated representative
Transition-In Plan	NLT 15 days following award of the Task Order
Transition-Out Plan	NLT 180 days prior to end of final performance period, or as otherwise directed by the COR

C.5.13.8 TECHNICAL EXPERT STATUS ACCREDITATION (TESA)

The Contractor shall be responsible for understanding and complying with DOD Contractor Personnel Office (DOCPER) TESA requirements. The Contractor shall submit completed TESA documentation to the GSA COR including: contract notification form, job descriptions, employee TESA applications, employee resumes, and employee employment contracts. After review and approval the GSA COR will submit all TESA documents to DOCPER for approval.

Note: DOCPER information and resources can be obtained at:
http://www.eur.army.mil/g1/content/CPD/docper.html

C.5.13.9 ACCOUNTING FOR CONTRACT SERVICES – U.S. ARMY MANPOWER REPORTING

The Contractor shall report manpower data identified below under EUCOM's Unit Identification Code (UIC) and AFRICOM's UIC, as applicable.

The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collections site where the Contractor shall report ALL contractor manpower (including subcontractor manpower) required for performance of this contract. The Contractor is required to completely fill in all the information in the format using the following web address https://cmra.army.mil . The required information includes:

1. Contracting Office, Contracting Officer, Contracting Officer's Representative
2. Contract number, including task and delivery order number
3. Reporting period will be the period of performance not to exceed 12 months ending September 30 of each Government fiscal year and must be reported by 31 October of each calendar year. Contractors may direct questions to the help desk at contractormanpower@hqda.army.mil, or https://cmra.army.mil/Helplhelp.html.
4. Uses and Safeguarding of Information. Information from the secure web site is considered to be proprietary in nature when the contract number and contractor identity are associated with the direct labor hours and direct labor dollars. At no time will any data be released to the public with the contractor name and contract number associated with the data.
5. Estimated direct labor hours (including subcontractors)
6. Estimated direct labor dollars paid this reporting period (including subcontractors)
7. Total payments (including subcontractors)
8. Predominant Federal Service Code (FSC) reflecting services provided by contractor (and separate predominant FSC for each subcontractor if different)
9. Estimated data collection costs
10. Organizational title associated with the Unit Identification Code (UIC) for the Army Requiring Activity (the Army requiring Activity is responsible for –providing the contractor with its UIC for the purposes of reporting this information.
11. Locations where contractor and subcontractor perform the work (specified by zip code in the United States and nearest city, country, when in an overseas locations, using standardized nomenclature on website
12. Presence of deployment or contingency contract language
13. Number of contractor and subcontractor employees deployed in theater this reporting period (by country).

C.5.13.10 TASK ORDER TRANSITION

The incoming and outgoing contractors shall work together, in collaboration with the Government, to rationalize Transition-In and Transition-Out Plans to effect a transition that provides for smooth operational turnover which minimizes operational impact to supported organizations.

C.5.13.10.1 KICKOFF MEETING

The Contractor shall participate in a Kick-Off Meeting with the Government at a time and place scheduled through the GSA Contracting Officer, or designated representative. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved in administration of the Task Order. The meeting will provide the opportunity to discuss contract transition; technical, management, and security considerations; reporting and deliverable submission procedures; travel/tool/ODC approval processes; billing/invoicing procedures, etc. At a minimum, the attendees shall include key contractor personnel, representatives from, key Government personnel from the stakeholder organizations, and representatives from GSA's Contracting Office.

C.5.13.10.2 TRANSITION-IN PLAN

The Contractor shall prepare, for review and approval of the Government, a Transition-In Plan that includes a schedule depicting the transition activities and milestones for accomplishing the Task Order transition.

The Contractor shall perform the following activities during the transition-in period:

- Perform joint inventories and inspections of all furnished facilities and property with the government and outgoing contractor.
- Perform joint identification and inventory of all contractor maintained classified data, equipment and devices relevant to the performance of the contract, to ensure that proper accountability and chain of custody is maintained for all COMSEC sensitive items.
- Develop and validate a comprehensive communications and IT supported equipment list with the government and outgoing contractor.
- Coordinate with the government to validate or establish Mission Assurance Categories (MAC) and maintenance priorities for supported equipment.
- Establish procedures with the outgoing contractor to transition operations, maintenance, and logistics functions while maintaining an uninterrupted continuity of services without a degradation of service. This includes defining processes for turnover of system administration, accounts, privileges, and access.
- It is anticipated that weekly status meetings with all pertinent stakeholders at a mutually agreed upon day and time will be conducted.

It is anticipated that joint status meetings with pertinent stakeholders will be held at a mutually agreed upon dates and times.

C.5.13.10.3 TRANSITION-OUT PLAN

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to the incoming contractor/government personnel at the expiration of this Task Order. The Contractor shall develop, document, and provide a Transition-Out plan NLT 180 days prior to the Task Order end date or earlier if directed by the Government. The Contractor shall identify transition activities, schedules and milestones for turnover of work centers/functions and identify how it will coordinate with the incoming and or Government personnel to transfer knowledge regarding the following:

- Project management processes.
- Points of contact.
- Location of technical and project management documentation.
- Status of ongoing technical initiatives.
- Transition of personnel.
- Establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition.
- Inventory, inspection and transfer of IT software and hardware, licenses, and warranties.

- Inventory, inspection and transfer of all contractor maintained classified data, equipment and devices, ensuring positive control, accountability, and chain of custody is maintained for all COMSEC sensitive items.
- Technical artifacts and configuration baselines.
- Elevated system privileges, i.a.w. technical direction issued by the COR and DAA/AO.
- Operations, maintenance, helpdesk, engineering and logistics functions.
- Mission Assurance Categories (MAC) and maintenance priorities for supported equipment.

OPTIONAL REQUIREMENTS IN THIS SECTION WILL BE FUNDED AT THE TIME EXERCISED.

C.6. OPTIONAL SERVICES

The Government reserves the unilateral right to exercise the following optional services. Options will be invoked through award of a Task Order modification issued by the Contracting Officer. Options may be invoked, in whole or in part, at the discretion of the Government. The Contractor will be provided 60-days from time of option exercise to staff positions.

At the time of exercising an option, the Government will further definitize requirements, where necessary to:

a. Provide technical direction necessary to clearly delineate the extent of support and nature of work to be performed, deliverables and required timeframes, if any.
b. Specify technical details about the specific environment (e.g. network, systems, applications, tools) where support is required.
c. Identify place(s) of performance.
d. Define the business hours in which support is required and specify requirements, if any, for providing 7-days a week, 24-hour coverage or recall during non-business hours.
e. Identify required service level(s) and performance standards, if any.
f. Specify security clearance requirements.
g. Identify specific certification requirements of DoD Manual 8570.01M, Information Assurance Workforce Improvement Program applicable to the option being invoked.

C.6.1. COMMON OPTIONAL TASKS

Options described in PWS section C.6.1 may be invoked to support 5SC requirements or other DoD stakeholder organizations in PWS section C.2.2. Sites and Customer Base requiring services under this Task Order.

Optional positions are anticipated to include technical skillsets similar to the labor mix performing the mandatory services under this Task Order.

For proposal purposes, the Not-to-Exceed (NTE) value of this option is $___TBD___ per year. For proposal purposes, include a labor mix consisting of the requisite skillsets needed to perform the work described in PWS sections C.6.1.1 thru C.6.1.5 below. The Government seeks an optimal mix of labor that provides the requisite skills to perform the work in a high quality, cost-effective manner.

C.6.1.1. ENGINEERING & INSTALLATION (E&I) SERVICES (OPTIONAL)

During this Task Order, it is anticipated that the Government may require optional engineering and installation (E&I) services to support specific projects to consolidate infrastructures; application migration; upgrade or replace legacy technologies; perform technology insertions; extend, enhance or modernize networks, systems, and communications capabilities; standardize configurations; streamline network operations; or improve the security posture of the technical environments supported under this Task Order. Specific E&I requirements will be definitized at the point of exercising an option.

It should be noted that as the 5SC undertakes transformation initiatives to fully realize the visions for the Joint Information Environment (JIE) and Joint Enterprise Network (JEN), the E&I projects that arise under this optional task, may be driven in whole or in part by the 5SC or any of the stakeholder organizations benefitting from the services provided under this Task Order:

a. The technical boundary for this optional work encompasses the transport layer and footprint of existing networks/systems and extensions of such.
b. The geographic boundary for this work encompasses support of DoD organizations located in the European theater or African theater that are migrating to the JEN/JIE.

If exercised, the Contractor shall, consistent with the definitized E&I requirements:

- Provide documentation and technical input for decision briefs, architecture, engineering, implementation, and migration plans.
- Perform technical site survey(s) to capture and validate conditions and site specific requirements to plan and design the project. When specified by the Government, this includes producing a technical assessment of the level of effort for performing the work and preparing a Bill of Materials with an itemized list of all required components (hardware and software) and ancillary items needed for the project with their associated costs.
- Prepare an E&I Project Plan defining the scope, schedule, and resources needed to execute the E&I project.
- Produce engineering designs, specifications, and/or drawings to meet the specific project requirements, ensuring that solutions are designed for compatibility and interoperability.
- Coordinate the establishment of circuits (where required) with physical and logical redundancy and sufficient bandwidth to meet network/system quality of service requirements.
- Perform integration, installation, and final configuration services.
- Install, configure, and integrate requisite components and ancillary items.
- Develop, track, and update test documentation. Perform testing of all circuits, equipment, and components to ensure proper configuration and operation.
- Develop and implement migration plans in a manner that minimizes negative operational impact as much as possible.
- Produce/update system documentation, drawings and configuration records on the installation and integration of all components.
- Conduct knowledge transfer and training as part of turnover activities.
- Provide operations, maintenance and sustainment services where ongoing support requirements are specified in the option notice.

C.6.1.1.1 EUCOM's Commercial Solution for Classified (CSfC) Pilot

EUCOM has a requirement to modernize the remote access capability utilizing commercial solutions to replace the traditional Type I CCI to encrypt the transport of classified data. The Suite B CSfC has been used by other DOD organizations to satisfy this requirement. CSfC utilizes Commercial Off-The-Shelf (COTS) equipment in a layered architecture and utilizes public domain algorithms to satisfy the Information Assurance controls that are mandated for providing transport of classified networks.
The Contractor shall:

- Design, document, and implement a working CSfC solution that can be turned into a repeatable process for integration into the EUCOM environment
- Leverage IA documentation and network architecture diagrams as well as 'lesson learned' from other DoD approved CSfC solutions to expedite the effort at EUCOM
- Complete all required documentation for IA accreditation and shepherd the pilot solution through the Authorizing Official approval process.

Request completion date is o/a 15 Nov 2014. Special contract requirements as described in paragraph H.3 Security and H.5 Personnel Qualifications apply to this work.
Deliverables:

- Engineering Plan
- Architectural Drawings
- Configurations and settings
- Test Plan and Results
- Required IA Documentation

CSfC Implementation
SCOPE:
Previously in Mod 5 EUCOM commissioned the Contractor to design a CSfC Pilot as a proof of concept. Based upon the pilot's outcome and lessons learned, EUCOM has decided to move forward with the implementation of CSfC in a limited capacity for SIPR access in designated General Officer Quarters as well as approximately 100 traveling kits.

TECHNICAL AND FUNCTIONAL REQUIREMENTS:
Specifically, the Contractor shall:

- Build, test, and implement a NSA approved CSfC capability for use projecting the EUCOM SIPRNet environment. Specific tasks include:
  - Building and implementation of the head end instance
  - Building and implementation of the 5 home kits to General Officer Quarters
  - Building and provisioning of 10 traveling kits (5 Laptop & 5 Tablet)
  - Build out of the Unified Computing System to support the ESXi virtual environment
  - Completion of all IA engineering tasks to include validation of all controls, developing/obtaining all required documentation, and completing the NSA Checklist
- Develop and document processes, procedures, and TTPs for the following requirements then train the Government identified service provider on their usage
  - End user training and documentation requirements
  - Certificate Authority creation and management
  - Head-end operation and maintenance requirements
  - Provisioning of the home kits, laptop travel kits, and tablet travel kits
  - Unique IA requirements associated with CSfC

OTHER INFORMATION:

- Period of Performance is upon modification issuance through o/a 6 Mar 2015. Special task order requirements as described in paragraph H.3 Security and H.5 Personnel Qualifications apply to this work.
- Deliverables:
  - As-Built Drawings

  - Configurations and settings
  - TTPs and Process Documentation
  - Required IA Documentation

- NOTE: This work is for the Implementation phase only, the Government has yet to publish a CONOPS (or define how and who will be performing the O&M) for CSfC.

C.6.1.1.2 EUCOM's SSO Database Upgrade

EUCOM requires the SSO database to be upgraded to EUCOM standard technologies (Microsoft.net and SQL 2008). The Contractor shall validate existing application requirements and gather new requirements; rewrite/upgrade existing application; integrate the new application into the EUCOM environment; and migrate current data to the application.

Deliverables required are:

- Project Plan
- Application Requirements Document (requires Gov't sign-off)
- Application Source Documentation (code, data mapping, schema…etc)

C.6.1.1.3 SOCAF J2 VTC E&I Services

General information.

All rooms in this scope are on the third floor. Existing control and AV matrix systems reside in the third floor TR, room 301. The offices on the third floor are comprised of sheet rock wall construction, with acoustic drop ceiling and solid concrete floor. The rooms have Europe style horizontal Panduit throughout. There are ample electrical outlets to support the effort. This effort is not expected to affect HVAC or lighting. The existing matrix switches and control systems shall be used to the greatest extent possible. The proposed solution shall use the existing horizontal fiber optic cable plant to the greatest extent possible; however additional cable runs will be required. Proposed systems equipment and control programming deliverables shall conform to AFRICOM – SOCAF standards.

Rm 306 Director's office requirement:

C. Install 1ea new 55 inch NEC LCD display on the left wall in the same location as the existing white board. The display will include side speakers which will serve as the room audio system. The room shall be configured to push the existing SIPR PC to the LCD, with the addition of: quad video, a new IPTV tuner, and three new JOC feeds. The room will be controlled via a single GFE, CV-10 AMX touch panel. The control and matrix switching will be added to the existing rm 304 infrastructure, the control program will be updated to the current SOCAF standard.

305 SAR Requirement:

Add one new NEC 55 inch display to the existing array of three displays in the front of the room. Move and re-install 1ea 55 inch NEC LCD display from room 318, mount on the right wall near entrance as a standalone system monitor, not connected to the control system. Add quad video, add three new JOC feeds. The quad and JOC feeds shall be routable to all displays. Reconfigure control and audio using the existing equipment, and updating to the current SOCAF standard.

304 Conference room requirement:

Update the AMX programming code to current AFRICOM-SOCAF standard. All equipment is to standard in this room with the exception of the classification signage. The existing signage shall be updated to the LG digital graphics.

321 Bay 1, 318 Bay 2.

Back ground: This space has eight 55 inch NEC displays, only five of which are connected to the AV system. There are two existing touch screens currently functional. There are nine functional PC feeds using Extron Fox 500 Transmitters. There is an existing half rack and the following extra disconnected components: 1ea CVC-10 AMX touch panel, (11ea Extron Fox 500 Transmitters), (3ea Extron IPLT T PCS4).

Requirement: Add three additional Extron Fox 4G receivers for the displays, so that all eight displays are routable destinations. Re-install the 20 existing Extron Fox 500 Transmitters at the desired location. (User shall provide a list or which PC's shall be transmitted to the AV system). Reconfigure the system so that all three touch screens are functional. Troubleshoot and fix existing scaling issues with the three center displays. Move existing IPTV receiver (currently on desk top) to the AV system as a routable source. Add quad video, routable to all displays. Tweak - tune - reuse, existing two zone audio system, 2ea existing IPTV receivers and remove existing DVD player. Update existing control programming code to current AFRICOM – SOCAF standard.

Final system will have the following:

- 20ea routable PC sources.
- 3ea routable IPTV receivers.
- 3ea touch panels.
- 2 zone audio system.
- 4ea JOC feeds.
- 8ea routable display destinations.
- 1ea quad video processor, routable to all displays.

Deliverables:

Installation Design Plan (IDP) compliant with AFRICOM – SOCAF standards.

New AMX control programming baseline.

As-built design package.

Systems acceptance test document.

Equipment manuals for all new components installed.

C.6.1.2. TIER 3 CUSTOMER SUPPORT ADMINISTRATORS (CSA) (OPTIONAL)

During this Task Order, it is anticipated that the Government may require Tier 3 Customer Support Administrators to be exercised at the Government's discretion in order to provide focalized technical services and end user customer support to a specific building or specialized faction of users. The purpose of this option is to provide more accessible support to a targeted part of the populace.

For proposal purposes, include pricing for optional Tier 3 CSAs with the technical skills to perform the work described in this section based on a 1,860 hour man-year in each year of performance.

If exercised, the Contractor shall provide desk-side touch and application support services for IT end user device issues to assigned building and/or customer base. The Contractor shall provide immediate desk-side service to mission critical users for IT related issues which may include:

- Problem recognition, research, isolation, resolution, tracking, and follow-up.
- Tier 2 support to end users for desktop, thin client, network, applications, or hardware
- Coordinate and interact with the IT service provider.
- Recommending hardware, software, and modifications to meet end user requirements and/or mitigate issues.
- General touch labor support.

Under this option, the Contractor may be required to develop alternate work schedules for review and approval of the Government and provide support during work hours that fall outside of the normal duty hours of Monday through Friday 0800-1700. Contractor employees shall be dedicated to assigned building and consider the building as their prime work locations. At the time of exercising the option, the Government will specify the:

- Required work hours and where applicable, any on-call requirements associated with this support.
- Building locations and/or customer base where required CSA services are required.

C.6.1.2.1. AFRICOM COMMAND CONFERENCE ROOM CSA

The Contractor shall provide Subject Matter Expert level support for the USAFRICOM Office of Shared Services, Command Conference Center with Visual Information and Presentation services. Services shall be limited to operator functions to include user maintenance and assisting 5SC technicians (or outside agencies) troubleshooting malfunctions. Systems supported include:

- AMX touch panel
- Tandberg C60/C40 st
- Jupiter video splitter
- Annotator
- DIS/Shure translation System (Microphones), audio mixing
- SmartBoard
- Christie Projectors
- Vbrick IPTV endpoints
- Defense Connect On-Line (DCO)
- Unified Communications (UC) (e.g. Lync, VOIP, VoSIP, etc.)

The SME primary duties shall be to serve as the primary point of contact for Command Conference Center Information Technology (IT) support to the Combatant Commander and Senior Staff, supporting Bldg 3312 and 3306. The SME shall perform conference scheduling, set up and operations, and assisting end users in operating A/V and end-user automation equipment. The scope of this support includes:

- Maintaining and troubleshooting end-user AV equipment
- Coordinating multi-session VTC bridging with 5SC technicians and external participants
- Using and troubleshooting:
  - Unified Communications (UC) capabilities (e.g. Lync, DCO, etc.)
  - Projection and sound equipment

- As well as performing other related technical and administrative tasks in order to enable connectivity both with internal and external participants

As time allows, secondary duties shall include performing as the Office of Shared Services, Customer IT Services technician for desktop related problems (see paragraph C.5.3.1.3 for detailed description of services).

C.6.1.2.2. CLDJ CUSTOMER IT SUPPORT SERVICES

The Contractor shall provide 4 FTEs to provide desk-side touch and application support services for IT end user device issues connected to CLDJ networks require support under this contract. The Contractor shall provide immediate desk-side service to mission critical users for IT related issues which may include:

- Problem recognition, research, isolation, resolution, tracking, and follow-up
- Tier 2 support to end users for desktop devices (ie computers, laptops, printers, VOIP phones…et.) and associated application
- General touch labor support to include installation of devices

Normal duty hours are defined as Monday through Saturday 0800-1900 (10-hour days with an hour lunch)

C.6.1.2.3 EUCOM DCOM CUSTOMER IT SUPPORT SERVICES

The Contractor shall provide the DCOM and his staff desk-side touch and application support services for their IT end user devices to include supported mobile devices. The Contractor shall provide immediate desk-side service to mission critical users for IT related issues which may include:

- Problem recognition, research, isolation, resolution, tracking, and follow-up
- Tier 2 support to end users for desktop, thin client, network, applications, or hardware
- Coordinate and interact with IT service provider
- Recommending hardware. software, and modifications to meet end user requirements and/or mitigate issues
- General touch labor support

This requirement may require the Contractor to provide support during Command Operations that will require work hours falling outside of normal duty hours therefore alternate work schedules. Normal duty hours are defined as Monday through Friday 0800-1700.

C.6.1.3. INFORMATION ASSURANCE SUPPORT (OPTIONAL)

During this Task Order, it is anticipated that additional Information Assurance positions may be needed in the base and each option year to support increased information assurance services to support potential growth in this area of the task attributable to requirements.

For proposal purposes, include the following optional IA positions with the technical skills to perform the work described in this section based on a 1,860 hour man-year in each year of performance:

Optional Support
• **IA Senior IT Analyst**
• **IA Senior Technician**

- **IA Technician**

The scope of this optional task includes performing information assurance, certification and accreditation, computer network defense, vulnerability management and remediation activities and related work similar to the requirements described in PWS sections C.5.3.5 through C.5.3.5.3. Specific IA requirements will be definitized at the point of exercising an option.

The work under this option may be performed under the purview of the 5SC DAA/AO, 5SC IAM, or other designated approval authority specified at the time of exercising the option

C.6.1.3.1 AFRICOM INFORMATION ASSURANCE COMPLIANCY MONITOR

The Contractor shall perform as the AFRICOM Compliancy Monitor to ensure AFRICOM networks are compliant with the DoD Information Assurance Vulnerability Management (IAVM) Program. The Compliancy Monitor is primarily an auditing function used to validate that all AFRICOM network assets are compliant regardless of who are the system owners (who manages/administers them). The Contractor shall provide the following support and services:

- Evaluate and implement all applicable Information Assurance Vulnerabilities, Bulletins and Technical Advisories i.a.w. CYBERCOM directives. Track CYBERCOM Command Tasking Orders (CTOs), FRAGOs, INFOCON; Coordinated Alert Messages (CAMs), and other directives for AFRICOM network assets. Perform analysis, implement, and report the compliancy of Information Conditions (INFOCON) changes and Communications Tasking Orders (CTO).
- Manage Vulnerability Management System (VMS) for AFRICOM to include:
  - Populating all AFRICOM network assets (comprised of 5SC, POR, and Contractor managed systems), establishing "buckets" as needed, and entering data as required
  - Ensuring appropriate VMS entries have been made for STIG compliance
- Perform System Administration (O&M) and manage Assured Compliance Assessment Solution (ACAS) servers as a service
- Ensure all applicable IAVMs are entered into the 5SC ticketing system (currently NSS)
- Perform vulnerability scans on all AFRICOM network assets using ACAS. Reconcile scan results with VMS and:
  - Update compliancy in VMS (as necessary) for those system which the scan show compliant or
  - Update the ticket to notifying system owner/SCCM of non-compliant systems or
  - Create a new ticket if the original was closed and the scan shows non-compliant

  (Note: System owner is defined as the organization responsible for system administration)
- Maintain a list of applicable Security Technical Implementation Guides (STIGs). Reconcile with DISA STIGs to determine if updates/changes have occurred. Review updates/changes to determine impact the AFRICOM network assets and open ticket to notify the system owner of any required action
- Manage the DoD ports, protocols, and services management (PPSM) program for AFRICOM. Track and document approved "opened" ports and protocols inbound and outbound using the appropriate DOD approved tool.
- Report IAVM, CTO, FRAGO, INFOCON and CAM compliancy weekly using a Contractor develop, Government approved format to the AFRICOM IAM/DAA
- Perform unscheduled (adhoc) scans using ACAS at the request of the IAM and provide scan results/reports. Adhoc scan requests are not to exceed 10 per calendar month.

(Note: DOD is transitioning from VMS to Data Management and Reporting System (DMRS) which will receive automated updates directly from ACAS. Impact to processes and staffing needs will need to be re-evaluated once the transition occurs.)

C.6.1.4. NETWORK MANAGEMENT, SYSTEMS ADMINISTRATION, DATABASE SUPPORT (OPTIONAL)

During this Task Order, it is anticipated that additional network, systems administrators, or database administrators may be needed in the base and each option year to support network management, systems administration, or database administration requirements that extend beyond the work included in the mandatory services described in PWS section 5.

For proposal purposes, include the following optional IA positions with the technical skills to perform the work described in this section based on a 1,860 hour man-year in each year of performance:

Optional Support
• Sr. Network Specialist (Senior)
• Network Specialist (Journeyman)
• Systems Administrator (Senior)
• Systems Administrator (Junior)
• Database Administrator, Senior (SQL)
• Database Administrator, Journeyman (SQL)

If exercised, the scope of this optional task includes performing network management, systems administration, data analytics, and/or database administration services similar to the requirements described throughout PWS sections C.5. Specific requirements will be definitized at the point of exercising an option.

C.6.1.4.1 AFRICOM Campus DSL Network Management Services

AFRICOM's Campus DSL (CDSL) provides centrally managed, commercial internet access to approved user/devices located on Kelly Barracks, Stuttgart, Germany. The commercial circuit enters Patch Barrack in Building 2375 before going to the border router in building 2383. The service is then encrypted and routed over 52nd Sg Bn dark fiber to Kelly Barracks Building 3304 where it is broken out and distributed to the various buildings requiring service.

The Contractor shall provide O&M services for the designated network devices within the Campus DSL Accreditation Boundary (see Attachment B.1 AFRICOM CDSL System Overview) and the associated Network Management System. Currently, the CDSL network supports approximately 80 connections in 7 buildings with expected growth not to exceed 200 connections and 10 building only on Kelly Barracks. Contractor services shall be limited to the designated network devices only on Patch and Kelly Barracks, there shall be no end user support required other than configuring the ports to accept the end user devices.

The CDSL network is designated as a Mission Assurance Category III system with a Maintenance Priority of 4 (see para C.5.1.5.1 & C.5.1.5.2 for details). As such, services will only be required Monday thru Friday from 0800 to 1700 excluding US Federal Holidays. No after hour support is required however the Government may adjust requested hours with 24 hour notice to support specific requirements provided the standard 40-hour work week is maintained.

Contractor personnel performing these services must possess a minimum of a SECRET clearance and meet 8570 requirements for an IATII with a minimum of a CCNA computing environment certification.

Specific services required are:

For O&M Tasks:

- Provide CDSL network connectivity by installing, configuring, maintaining, and troubleshooting end user building (EUB) devices (designated routers and switches)
- Allow only end user devices with an '*approval to connect'* from AFRICOM access to the network
- Patch EUB device port to the requested port of the building's distribution system within the TR
- Notify 5SC Service Center when:
  - Commercial internet services are not being received (e.g. circuit outages)
  - Support actions are required on the Area Distribution Node (AND) devices
  - Dark fiber circuit outages occur between Patch and Kelly

For Network Management System (NMS) tasks:

- Load the AFRICOM provided image on the NMS device and ensure changes to the image are approved by the AFRICOM CAB prior to installing
- Administer the NMS IAW paragraph C.5.2.1.1 Common System Administration Tasks and C.5.2.1.2 System Security Tasks to include ensuring the NMS is updated with the most recent anti-virus signature

For Network devices within the CDSL accreditation boundary tasks:

- Maintain all supported network devices within the CDSL Accreditation Boundary i.a.w. DISA STIGs, IAVAs, and CYBERCOM taskings
- Apply password control management and port security management processes
- Take appropriate measures to respond to known and possible network attacks i.a.w. applicable DoD policies, directives and instructions, or as directed by the CND Service provider
- Perform IA Compliance scanning of devices to include the NMS
  - Configure and maintain the scanning device
  - Conduct scanning of devices quarterly, update results in VMS, and resolve findings
- Coordinate with AFRICOM J62 to schedule an annual CNDSP external assessment
  - Acknowledge receipt of report and provide copy to AFRICOM J62
  - Resolve findings

For the boundary defense (firewall) device:

- Configure and maintain the firewall device IAW DISA STIGs
- Firewall ACLS shall be configured IAW approved AFRICOM CCB configurations
- Review logs and document completion IAW DOD and AFRICOM policies
- Provide audit and/or log files to the CNDSP upon request

C.6.1.5. TASKER MANAGEMENT TOOL SUPPORT (OPTIONAL)

During this Task Order, it is anticipated that the Government may require full-time Senior IT Analysts to support Tasker Management Tools implemented by stakeholder organizations supported under this Task Order. The scope of this optional support includes providing technical assistance with the installation, integration, configuration, and administration of the respective tools; maintaining the server and operating system; managing the database; providing database administration support to maintain the structure and integrity of the tool/data; providing for the operations and maintenance of the tools to ensure the operational availability and integrity of the data. Where directed, end user assistance in using the tool's functionality or troubleshooting problems may also be required.

For proposal purposes, include the following optional positions based on a 1,860 hour man-year in each year of performance:

Optional Support
• **Senior IT Analyst**

Support for the procurement of Tools consistent with the requirements described in Section H.2.4, titled "TOOLS - HARDWARE/SOFTWARE AND MISCELLANEOUS ODCs" or other related technical services consistent with requirements described in PWS section C.5 REQUIRED TASKS or defined when options are exercised, may be identified in technical direction provided by the COR.

At the time of exercising this optional support, the Government will identify the specific Tasker Management Tools or products requiring support and define any specialized requirements associated with this support.

C.6.1.6 EPOC-IOSAD Computer Network Operations SME

The Contractor shall provide Computer Network Operations Subject Matter Expertise to the European Plans and Operations Center (EPOC) - Information Operations (IO) Special Activities Division (IOSAD) in support of their efforts in forming capabilities and providing technical services to support the integration and synchronization of Theater IO efforts into current and future Operations Plans (OPLANs). The Contractor shall conduct mission and operational analysis that supports the spectrum of IO support through the planning and review of EW, Military Information Support Operations (MISO), Military Deception (MILDEC), Computer Network Operations (CNO), Operations Security (OPSEC) activities, as well as Strategic Communications (SC). The Contractor shall:

- Provide analysis for the development of procedures, organizations, and allocation of IO responsibilities and tasks to intelligence and operational organizations across the region
- Provide for the analysis and implementation of IO and STO tools and capabilities
- Support the design and insertion of IO activities into the USEUCOM Regional/Country Cooperation Plans (RCP/CCP)
- Support development of CONOPS and requirements for IO capabilities and programs that will enhance warfighting capabilities
- Provide options that utilize IO and STO capabilities to enhance current operations, crisis response, survivability, and force protection
- Provide support to the conduct of theater scenario exercises with Command elements utilizing strategic and operational IO capabilities

In addition, the Contractor shall provide Content Management to include end-user support services to the EPOC-IOSAD for their SIPR and NIPR Portal Environments. The Contractor shall be responsible for developing and maintaining the content baseline for the IOSAD's Portal pages, as well as converting and cataloging dynamic/non-standardized reports to ensure EUCOM and DOD users have access to these reports in a secure manner. The Contractor shall:

- Upload and manage the IOSAD's SharePoint content

- Serve as IOSAD’s technical lead for their portal activities by liaising between the IOSAD users and the Enterprise SharePoint team
- Troubleshoot (Tier 0) content-related issues, processes, user accounts, security issues, and procedures within enterprise SharePoint portal applications
- Perform as IOSAD’s Information Security point-of-contact for portal related security concerns to including maintaining a Cyber Security awareness on potential nefarious activities against the portal
- Advise the staff on proper document profiling and customization, streamline existing and/or design new methods/capabilities to manage the Division’s information, and provide user training to enhance IOSAD’s ability to distribute information
- Serves as the IOSAD’s Knowledge Management SME by liaising with EUCOM’s KM Team

C.6.1.6.1 AFRICOM JOINT OPERATIONS CENTER (JOC) PRESENTATION SERVICES

The Contractor shall provide O&M for AFRICOM JOC’s virtual device management systems and audio visual systems provided through the Thinklogical Audio/Visual equipment suite. Normal duty hours for JOC support are increased to Monday through Friday 0700-2200. When services are required outside of normal duty hours due to mission needs, the Government should provide at least 24-hour notice.

The AFRICOM JOC consists of several key areas including the Senior Decision Cell, the Watch floor, three Operation Center Rooms, three Action Cells, Conference Rooms, Team Rooms, Theater Rooms and Telecommunication Rooms.

[Note: Reference PWS Attachment B.11 AFRICOM JOC Conceptual Drawing for details.]

The Contractor shall:

- Provide O&M support, coordination, and monitoring for all systems related work in the JOC, including Audio Video (AV) routing matrix, computer systems, architecture, controlled lighting.
- As time allows, provide user training and over-the shoulder guidance for JOC personnel to ensure operational efficiency to include creating TTPs, SOPs and operational guides
- Develop and implement an operations check for the equipment/systems in the Senior Decision Cell. Report accomplishment and/or findings to the JOC Watch Officer NLT 0800 daily. *Note: Contractor performed daily checks are limited to the SDC only, all other areas are the responsibility of the user*
- Create and implement a Preventative Maintenance Schedule to maintain and prolong equipment life to include replacement of consumables IAW manufacturer recommendations
- Provide configuration/change management for the software code used to manage the ThinkLogical systems and AMX Control devices. Make user defined routine changes as required and provide capability for implementing major changes periodically
- Provide weekly status briefs on the JOC Audio-Visual Presentation systems and project status

Other:

- The Facility has been declared a Special Security Area therefore Contractor employees will require a Top Secret clearance with SCI access Security Clearance
- Contractor employees support the Audio-Visual (Presentation) requirement must have or obtain

within 6 months the Cisco CCNA Video as their 8670 Computing Environment certification with at least one FTE s with a minimum of 1 years experience in installing, operating, and/or maintaining ThinkLogical systems. Other certifications may be consider but are subject to Government approval. Finally while not a requirement, AMX programing experience is considered very desirable.

C.6.1.7 TSCMIS SERVICES

AFRICOM and EUCOM continue to use G-TSCMIS and the TREX back end with their related databases however have preceded on differing paths on what data needs to be present and how it is shown. Their divergent paths are further compounded with an immediate need to replace the front end applications and dashboards with software code that is current and supportable. Both COCOMs have decided to supplement their staff to meet their own individual needs.

C.6.1.7.1 EUCOM ENHANCEMENTS

Replace the Strategy of Active Security (SAS) Plan application (currently written using Silverlight) with a new tool written in Module View Controller (MVC) architecture and the .Net Framework. The functions performed by the tool shall remain basically the same however the Contractor shall work with Government representative to define enhancements as requested.

Redesign and replace the TSC Dashboard to interface directly with TREX databases to present the requested information in easy to understand views. Work will require using MVC architecture and redesigning the SharePoint front end.

Provide maintenance and sustainment to support these tools and provide continuous improvement to meet Government changing needs

C.6.1.7.2 AFRICOM ENHANCEMENTS

Continue development of the Integrated AFRICOM Theater Sync System (IATSS) application using Module View Controller (MVC) architecture and the .Net Framework. Enhance current capabilities (Version 1) to include capturing strategic direction (i.e., LOEs and IMOs), bilateral direction (i.e., fully digital CCPs), and aligning Security Force Assistance capability packages, TSC projects, and resources.

Develop capabilities (Version 2 through 4) to enable operations objectives and aligned resources tracking, exercise objectives and aligned resources tracking, strategic and performance assessment tracking, TSC proposal life cycle management, and a NIPR capable version of IATSS.

Provide maintenance and sustainment support these tools and provide continuous improvement to meet Government changing needs.

C.6.1.8 FLAGSHIP Services

The Contractor shall provide engineering and O&M service for FLAGSHIP by performing the following functions:

- Network and system engineering to include completion of the DAR amd implementation of the Mobile Asset capability packages. In addition, should time allow, the Government may request integration CSfC into the Executive Communication Kits.
- Network and System Administration of FLAGSHIP as described in section C.5 to include performing certificate authority duties for both the red and grey networks.
- Service desk response for all Flagship calls to include triaging incidents and problem elevation
- Perform as the Flagship Security Auditor which in addition to Information Assurance tasks described in PWS paragraph C.5.4.9 specific tasks include:
    - Conducting NSA Required Weekly Compliance Auditing
    - Use the Dell Data Protection Encryption to manage DAR solution
    - Audit and maintain End User Device agreements
    - Perform all CND functions for the CSfC network to include incident handling, response, and reporting. (Note: Report all incidents to the EUCOM AO (or IAM) and the designated NSA POC)

OTHER INFORMATION:

- One individual cannot perform Certificate Authority duties for both networks on a single request
- The Security Auditor is only authorized access to audit logs and may not perform system administration duties on the CSfC grey network or as a Certificate Authority on either network
- The Contractor shall be responsible for the FLAGSHIP network, SIPR services accessed by the end user, and the end user device to include the baseline software. End user CSfC connection provisioning to include documentation and training, along with end user support for connecting the devices is the responsibility of the designated Government entity.

C.6.2. AFRICOM SPECIFIC OPTIONS

Options described in this section may be invoked to support AFRICOM-related requirements.

C.6.2.1. COMPUTER NETWORK DEFENSE (CND) (OPTIONAL)

During this Task Order, it is anticipated that the Government may require additional contractor support to provide optional Computer Network Defense Services.

For proposal purposes, include 2 optional CND positions based on a 1,860 hour man-year in each year of performance.

If exercised, the Contractor shall provide the following support and services:

- Implement measures to prevent unauthorized software from being installed and executed on systems.
- Archive, monitor and review system audit logs and all other pertinent log files that will support incident response activities.
- Monitor all network anomalies (e.g. unauthorized network access, etc.) that occur on assigned networks.
- Develop and manage incident response actions (e.g. Tactics, Techniques and Procedures)
- Develop and recommend internal policies and procedures for handling network related incidents and protecting networks.

- Support incident reporting activities in accordance with CND Tier 2 policies and directives. Collaborate and interface with external organizations/agencies on security related issues and investigations. Report incidents to the, AFRICOM J62, AFRICOM ACCC, and the DAA/AO.
- Take appropriate measures to respond to known and possible network attacks in accordance with applicable DoD policies, directives and instructions.

C.6.2.2. AFRICOM DATA SHARING NETWORK (ADSN) Support at CJTF-HOA (OPTION)

During this Task Order, it is anticipated that the Government may require support for the AFRICOM Data Sharing Network (ADSN) hub and remote site SATCOM terminals (network infrastructure, SATCOM connectivity, ADSN systems, and High Assurance Internet Protocol Encryptors (HAIPE)).

For proposal purposes, price the labor mix necessary to provide the optional support described below.

The remote terminals provide tactically deployed users with connectivity to the ADSN data currently stored at CJTF-HOA. The ADSN network will be expanded soon to include a 2nd data center at RAF Molesworth; after this is completed, data may be accessed from either location via the ADSN network. The 2nd data center management at RAF Molesworth is out of scope for this Task Order, but troubleshooting the CJTF-HOA side of the terrestrial circuit linking the two sites is in scope. Each terminal provides the capability for multiple laptops/VOIPs to access services. The ADSN may be comprised of several terminal variants, operating in the Ku and Ka bands. The hub serves as a downlink site using a Rockwell Collins Deployable Ku band Earth Terminal (DKET).

There are 14 planned remote sites planned with a minimum configuration of two workstations, two VOIP phones, and a printer at each remote site. There are 4 U.S. workstations and 3 VOIP phones at the hub (Camp Lemonnier).

Note: This is a needs based network and the number of nodes/locations could grow or change, dependent on mission needs of the Government and partner nations. The Contractor would be expected to scale support under this option based upon actual need at the time of exercising the option. For proposal purposes, Offerors are advised to price the solution on the basis of the information presented in the PWS.

If exercised, the Contractor shall, consistent with technical direction provided by the Government:

a. **Operate and Maintain ADSN Coalition Tactical Baseband.** All support for the following items will be on site at Camp Lemonnier, Djibouti (CLDJ).

The Contractor shall maintain network baseband (switches, routers, call manager, circuits) to include HAIPE in-line encryptors. The hub network includes:

(1) A Cisco call manager express (CME) to broker hub and remote node VOIP calls.
(2) Hub equipment at one or more DKETs.
(3) Network infrastructure, PCs, printers, and VOIPs at Camp Lemonnier.
(4) A GFE terrestrial circuit from CLDJ to RAF Molesworth.

The Contractor shall:

- Maintain/integrate WAN accelerators and inline encryptors.
- Provide network administration for VOIPs and PCs.
- Assist military team(s) with key management and key loading as requested.
- Provide Over-The-Air-Rekeying (OTAR) services to remote nodes.
- Upon request, maintain a link to remote data center via a DISN transport circuit. This link will use separate GFE HAIPE encryptors.
- Train U.S. military personnel on O&M of hub infrastructure equipment on request of the TPOC.

- Provide touch maintenance support to US BICES program office, which will be operating the new data center at RAF Molesworth.

b. **Operate and Maintain Coalition Tactical User Equipment (Remote Sites).** It is anticipated that most of the following items shall be supported remotely, but the Contractor may be requested to travel to a Partner Nation site to help troubleshoot/restore service on-site.

The Contractor shall maintain network remote terminals (switches, routers, call manager, links) to include HAIPE in-line encryptors. The remote site network includes:

(1) A local Cisco call manager express (CME) to broker local VOIP calls and interface with hub call manager.
(2) Partner Nation PCs, VOIPs, and printers.
(3) SATCOM communications terminals.
(4) Baseband equipment.

The Contractor shall:

- Maintain/integrate WAN accelerator and inline encryptors.
- Assist military team with key management and key loading as requested.
- Maintain interoperability between remote sites and CLDJ's existing SATCOM transport environment.
- Train U.S. military personnel on O&M of remote node equipment upon request of the COR.
- Train coalition partner personnel on setup and use of remote nodes upon request of the COR. Training under this option will occur at CLDJ.

c. **Provide General Operations and Maintenance Support.**

The Contractor shall:

- Perform (or provide procedures to the operators to perform) regular preventative maintenance to ensure unscheduled outages are minimized.
- Actively monitor the network and workstations to proactively find and fix faults and ensure steady-state operations by ensuring the ADSN network continues to work as designed.
- Provide help desk support as the Tier 2/3 ADSN network Subject Matter Expert and being responsive to customer incidents 24 hours a day. Interface with US BICES program office coalition help desk to exchange tickets with US BICES/IIP that pertain to core services provided by the US BICES program office. Provide touch maintenance on behalf of US BICES program office technicians at CLDJ upon request.
- Maintain network diagrams and maintain IP plan, routing map/architecture, VOIP dial plan, and naming convention plan for the ADSN network.
- Patch infrastructure devices to mitigate known vulnerabilities or upgrade capabilities. Coordinate patch installation in advance with the US BICES program office. Ensure patching is done during periods of low operational network use IAW existing AFRICOM Authorized Service Interruption (ASI) procedures.
- Apply DISA STIGs, industry best security practices, and Information Assurance controls as directed by the DAA/AO to all network infrastructure devices and workstations upon request of COR.
- Coordinate warranty repair or replacement services for components of the ADSN network with vendors, as needed.

- Maintain infrastructure software version(s) and operating system information. Maintain the network configuration baselines using disciplined configuration management processes and procedures, consistent with the practices followed by AFRICOM, as described in PWS section C.5.3.6.1.
- Assist the Government in creating/maintaining a lifecycle management plan for the network.
- Assist the Government, where requested, with developing and implementing a disaster recovery program (that aligns with overall COCOM plans) to ensure continuity of operations. This will require coordination with the US BICES program office for their core services piece.
- Install new US ADSN workstations and VOIPs on CLDJ as requested by the COR.
- Install and provide touch maintenance for ADSN servers physically located at CLDJ, but remotely maintained by the US BICES PMO.

Specific reporting requirements associated with the optional support are expected to include:

- Implementing reporting processes for security incidents and security audit events that affect (or could affect) the operation and management of the system.
- Preparing a written report at least once a quarter to document actions taken on the network, a summary of incident tickets, a summary of preventative maintenance performed, and recommendations on how to improve operation and security of the system.
- Meeting with CLDJ J6 personnel at least once a week to review current status of ADSN network, open high profile trouble tickets, and upcoming ASIs.

C.6.2.3. SIPR and NIPR PORTAL SUPPORT and SOFTWARE DEVELOPMENT (OPTIONAL)

During this Task Order it is anticipated that AFRICOM may need project management, software engineering, and operations and maintenance support for AFRICOM's SIPR and NIPR portal.

During this Task Order it is anticipated that AFRICOM may need project management, lifecycle software engineering and development services, help desk support, training, and portal operations and maintenance support for AFRICOM's SIPR and NIPR portal.

For proposal purposes, price the labor mix necessary to provide the optional support described below.

Note: AFRICOM's existing SIPRnet and NIPRnet portal is based on Microsoft SharePoint

Applicable Documents:

ACI 6000.06 USAFRICOM Software Development, Testing and Integration Guidance
ACI 5600.01 USAFRICOM Knowledge Management – Information Management Program
ACI 5600.03 USAFRICOM SharePoint Portal Policy and Governance

If exercised, the Contractor shall, consistent with Government technical direction, provide:

a. Program / Project Management support **to l**ead the planning and implementation of software development projects. This includes:

(1) Facilitating the definition of project scope, goals and deliverables through interaction with the stakeholders/customers in requirements gathering meetings.

(2) Developing a Project Plan, for Government review and approval, that defines as a minimum the: scope, goals, deliverables, schedule/milestones, resource requirements, and work breakdown structure (WBS) identifying project tasks.
(3) Managing the project and tracking project deliverables to facilitate completion of the work on time and within the established budget.
(4) Reporting status to stakeholders.
(5) Monitoring software development to ensure is it developed in accordance with ACI 5600.03 USAFRICOM SharePoint Portal Policy.

b. Enterprise Design, Development, Integration and Testing Services. This includes:
(1) Developing and advancing the top-level information sharing and fusion architectures of the USAFRICOM portals.
(2) Updating and maintaining SharePoint Portal architecture/design/taxonomy documentation
(3) Facilitating meetings and working with stakeholders to identify, prioritize, and plan baseline information sharing and fusion software development projects within the portal architectures.
(4) Applying software engineering expertise and software lifecycle development support for new and emerging requirements or for modifications/enhancements to the existing portal, programs/applications consistent with Government approval USAFRICOM initiatives.
(5) Integrating software designs and testing to verify and validate that operational code meets design (architecture) specifications.
(6) Processing system change requests i.a.w. the processes followed by USAFRICOM.

c. Release Management Services to Deploy the Upgrade Capability to the Portal(s). This includes:
(1) Performing Integration, checkout, deployment (release) and demonstrating upgrades to portal(s).
(2) Capturing, tracking and reporting status of trouble tickets which inform the resolution of emerging integration and/or performance issues across all software releases.
(3) Demonstrating portal capabilities as requested.

d. Portal Operations Support. This includes:
(1) Providing domain expertise associated with the utility of the portal in support of information fusion tactics and operating procedures across USAFRICOM and other communities/individuals whom are authorized portal access by the Government.
(2) Attending weekly staff meetings to ensure AFRICOM mission execution considerations are integrated with portal operations.
(3) Providing in-depth, customer support to users, on tools, access, and including associated interfaces (hardware and software) for portals.
(4) Provide local, on-site help desk support. Tracking trouble tickets i.a.w. established incident management processes and responding to user initiated portal trouble tickets, including Maintenance Priority I, Priority II, or Priority III incidents. Target Resolution Times for User initiated trouble tickets are:

Priority I level within 2 hours.
Priority II level within 24 hours.
Priority III level within 48 hours.

(5) Documenting repetitive trouble tickets to produce an end user FAQ document that is posted to and maintained on the portal.

(6) Building groups tailored to the needs of users, communities of interest (COIs), using the built-in capabilities that exist in the portals.
(7) Collecting and documenting requirements unable to be met by existing portal capabilities and provide to the Government.

C.6.2.4. ELECTRONIC RECORDS MANAGEMENT ADMINISTRATION (OPTIONAL)

During this Task Order it is anticipated that the Government may need application subject matter expertise to support and administer AFRICOM's SIPRnet and NIPRnet Electronic Records Management (ERM) Application.

Note: AFRICOM implemented Hewlett Packard's Total Records and Information Management (TRIM) system.

For proposal purposes, price the labor mix necessary to provide the optional support described below.

If exercised, the Contractor shall serve as the technical expert for all matters pertaining to records management and the secure operation of the TRIM electronic records management application. The work requires sound knowledge of research methods and data analysis techniques. The scope of this work includes:

- Creating and managing end user accounts, inclusive of: registering and troubleshooting user profiles to ensure login capability, impose access controls, verify credentials, and maintain controlled access to documents and content within the ERM application.
- Serving as the TRIM systems administrator.
- Training AFRICOM end users on the TRIM application and records management.
- Cataloging electronic documents into TRIM.
- Assist with the collection and preservation of official classified and unclassified records, electronic versions, relating to day-to-day and operational documents in a manner that meets governance and regulatory compliance requirements for records retention.
- Supporting problem identification and resolution.
- Responding to and providing timely resolution of trouble tickets providing Tier III technical support to resolve incidents
- Responding to incidents and providing technical support for the timely resolution of Tier III trouble tickets.
- Applying sound project management processes and technical expertise to support system hardware/software upgrades; configuration changes; and installation of patches/fixes.
- Working in cooperation with Command C4I Specialists, where requested, to translate business needs into functional and technical requirements to plan, design, test, and implement enhancements to extend application functionality.
- Providing consultative support, where requested, to develop and/or recommend standards for the Command's Electronic Records Management system.
- Providing expertise in the operation of the TRIM application to:
  - Assist users in the cataloguing electronic documents into the ERM application
  - Assist users with reading, arranging and describing official Command records.
  - Respond to formal and informal requests for documents, performing a variety of searches within TRIM to retrieve artifacts maintained in the system in various formats (e.g.: Microsoft Word, Portable Document Format, PowerPoint files; briefings, images, video, or sound file collections, etc.)
- Participating in Staff Assistance Visits (SAVs) and assisting with drafting SAV reports. The SAVs provide a comprehensive measurement of organizational compliance with all applicable records

management regulations, and provide formal documentation as to compliance, discrepancies, and suggestions for improvement.

- Assisting with and facilitating the review and collection of records accessed that have permanent historical value under title 44 United States Code, (U.S.C.) pursuant to the provision for automatic declassification in section 3.3 of E.O. 12958.

C.6.2.5. ENTERPRISE ARCHITECTURE SUPPORT (OPTIONAL)

During this Task Order, it is anticipated that the Government may require optional enterprise architecture and engineering subject matter expertise and consultative support to:

- Assist AFRICOM with the synchronization of enterprise architectures, strategic planning, program/portfolio management, and capital planning for USAFRICOM IT Investments.
- Assist USAFRICOM with institutionalizing processes for ensuring the synchronized development, approval, publication, and compliance with enterprise-wide IT guidance (i.e.,: architectures, prototypes, portfolio management, standards and policies) .
- Provide unbiased, objective, and sound technical recommendations and solutions.
- Assist the Government with planning and oversight of technology investments to ensure alignment with the DOD Architecture Framework (DODAF) and the USAFRICOM Enterprise Architecture implementation of this framework.
- Providing EA input to governance boards and the capital planning and strategic planning processes.

The nature of the work requires the application of Enterprise Architecture subject matter expertise, senior engineering and solutions architecture expertise, disciplined project management processes coupled with capability analytics and business process automation knowledge and expert level system administration services in the tools cited below. The architecture work is to be completed i.a.w. the standard DOD Architecture Framework (DODAF), Data Models, and Architecture data stored or retrieved from the Architecture Registries.

Applicable Reference Documents Include:

- DoD Information Enterprise Architecture (DIEA) http://dodcio.defense.gov/Home/Initiatives/DIEA.aspx
- Department of Defense Enterprise Architecture (EA) Modernization Blueprint/Transition Plan http://dodcio.defense.gov/Portals/0/Documents/Final%20DoD%20EA%20Modernization%20Blueprint_20110225%20rev%201.pdf
- DoD Architecture Framework (DODAF) http://dodcio.defense.gov/dodaf20.aspx
- DoD Information Technology (IT) Enterprise Strategy and Roadmap http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf

USAFRICOM has selected The Open Group Architecture Framework (TOGAF) as the EA methodology for the Command.

For proposal purposes, include a labor mix in each of the four option years that provides the specialized Enterprise Architecture expertise and requisite technical skills needed to perform the work described below. It is anticipated that a significant amount of the work will require highly specialized skills. Therefore at time of option exercise, the Government may require positions to be filled by contractors holding a Federated Enterprise Architecture Certification (FEAC™) Institute certification

[e.g.: Black Belt (BB) Certification Enterprise Architecture (CEA); or Enterprise Architecture Center of Excellence (EACO) Enterprise Architect Fellow; or TOGAF 9 or higher certification.]

C.6.2.5.1. ENTERPRISE ARCHITECTURE REQUIREMENTS

If exercised, the Contractor (consistent with the definitized EA requirements and technical direction issued by the Government) shall:

a. **Provide Technology Research and Development Support for Enterprise Architecture.**

This includes:

(1) Conducting unbiased research, providing development support, and testing new technologies identified by the Government.

(2) Preparing New Technology Recommendation Reports based on findings from the research and testing. Typical report content includes an analysis of the positive and negative impacts of the technology on the Joint Information Environment (JIE) IT Infrastructure and user.

b. **Provide Enterprise Architecture Technical Services.**

This requires applying a broad range of professional engineering services to support the development, fielding, and post-deployment support of EA products and services.

The Contractor shall, consistent with taskings and technical direction provided by the Government:

(1) Provide Enterprise Reference Architecture Support. The Contractor shall:

- Maintain Information Enterprise Architecture documentation using the CaseWise tool
- Develop new reference architectures; develop and maintain the objective architecture
- Support architecture initiatives; assess component architectures
- Attend meetings and serve as the EA representative; and
- Revise USAFRICOM policy.

(2) Develop and maintain the Information Enterprise Architecture (IEA), integrating future content, including services and reference architectures. The Contractor shall support the development of requirements to enhance the enterprise wide structure of the EA.

The IEA shall be maintained as part of the USAFRICOM Enterprise Architecture.

(3) Apply expert knowledge of the USAFRICOM EA and IEA to support development and implementation of IEA Compliance Mechanisms which form the basis for determining the extent that specific plans, programs, systems, processes, or functions comply with the IEA.

(4) Conduct EA Program Assessments and Staff Assistance Visits. This includes performing on-site visits to:

- Develop EA documentation with local subject matter experts
- Perform assessments of specific programs and publish written assessment reports to document the level to which the program adheres to the IEA
- Develop "As Is" architecture analyses.

[It is anticipated on-site visits may encompass periodic travel to CONUS, Europe, or Africa.]

(5) Develop, update and maintain the Enterprise Reference Architecture. This includes:

- Designing and developing future EA content (e.g., enterprise services, segment architectures, reference architectures, and solution architectures).

- Providing consultative support to align policy, guidance, and enterprise-level architectures; to ensure the creation of federated architectures; and to enable the realization of the Command's vision for an Information Enterprise.
- Documenting processes for developing Reference Architecture.

(6) Provide EA Governance Support to:

- Assist in implementing enterprise-wide governance processes/procedures that cut-across multiple technical disciplines and functional areas (e.g., EA, IT Standards, Interoperability/Information Sharing, IT investments and IT Infrastructure)
- Assist in creating strategy documents that are fully synchronized across critical stakeholder's needs, including the Intelligence Community and allied partners.

This work also includes:

- Participating on and interfacing with governance bodies; developing briefing slides, executive summaries, white papers, and memorandums.
- Recommending business process reengineering improvements
- Supporting continuous process improvement (CPI)
- Providing analysis and implementation support
- Developing recommendations and alternative courses of actions
- Evaluating the impact of legislative mandates and required activities.

(7) Requirements Management Dashboard, Analysis, and Liaison Support
This work includes:

- Developing tools and products to collect information on current "efforts"
- Providing analytical support to address requirements and capabilities
- Monitoring and making recommendations to foster better decision-making
- Managing interdependencies and monitoring of resource use to assess whether end user requests for tools/technologies support the Command missions.

Note: AFRICOM currently uses a customized SharePoint workflow and site.

(8) Support the Alignment of IT Investments with Enterprise Architectures
The Contractor shall assist with: ensuring that IT investments are aligned and compliant with appropriate Federal, DoD, Component and Functional EAs. Activities include:

- Developing guidance and instruction to improve IT investment management and reporting
- Providing data collection, input, draft guidance, and assistance for IT budget reporting as an integrated part of portfolio management process
- Identifying, reviewing and providing recommendations to address Federal and DoD requirements impacting the Command's ability to implement and align the Enterprise Architecture, IT investments, management and reporting processes
- Reviewing, analyzing and providing recommendations to enhance the efficiency of IT investments and compliance with applicable EAs.

(9) Support the development and implementation of the Segment Architecture that is used to provide guidance, rules, constraints, and standards for component architecture and solution architecture development.

c. **Provide Support for Command and Control (C2).**

This includes:

- Assisting with development and coordination of policy, guidance, architectural analysis, and documents that define the Common Operations Picture (COP) and Common Intelligence Picture (CIP) initiatives.
- Facilitating common approaches to:
    1) Enable on-demand, real-time visibility of the theater and GIG security and risk posture,
    2) Synchronize and align information policy, authorities, and responsibilities,
    3) Monitor development, integration, and implementation of IT capabilities,
    4) Foster Joint interoperable solutions,
    5) Provide access to data to support information management and situational awareness requirements, and
    6) Coordinate IT Operation process commonality.
- Supporting architecture development and the migration and integration of the architecture into the JIE Objectives Architecture.
- Assisting with improving EA methodologies and guidance to ensure architectures are used for decision-making at all levels across the life cycle and within and across portfolios.
- Conducting reviews of architectures and standards to assess compliance with an enterprise approach.
- Participating in the development of USAFRICOM's IE Strategic Plan, attending meetings and providing technical documentation (e.g. point papers) to support meetings, conferences, and working groups

d. **Provide Configuration Management Support.**

This includes providing support to develop and issue strategic guidance to assist AFRICOM with implementing an effective, disciplined configuration management (CM) process that align to 5th Signal's Configuration Management Plan, processes, and procedures.

e. **Observe the DoD Architecture Registry System (DARS) Road Map.**

f. **Provide Governance and Policy Documentation Support.**

The Contractor shall draft, review, recommend changes, and revise/re-write documentation (e.g. Directives, Instructions, and Command guidance, architecture views, diagrams, drawings, etc.). The Contractor shall brief the status and technical details of ongoing development and completed architecture work.

The primary method of tracking these tasks is through the Task Management Tool (TMT), a Microsoft Dynamics based application.

g. **Project Management (PM) Support.**

The Contractor shall provide centralized project management support to integrate, monitor and control interdependencies among the projects, EA, PfM, and Governance. The Contractor shall ensure that activities and processes are coordinated and integrated i.a.w. documented processes. This work includes:

- Definition and management of project management processes, project schedule, quality standards, measures and metrics, document configuration management; providing for centrally managed change; and tracking risks and issues.
- Applying an integrated, standards-based project management approach lifecycle,
- Balancing competing constraints of scope, quality, schedule; budget, resources, and risk while satisfying project requirements and addressing stakeholder expectations.

Project activities are recorded with the USAFRICOM Enterprise Project Management Server based on the Microsoft Project Server product.

h. **Portfolio Management Support.**

The Contractor shall provide portfolio management support to align investments with mission strategies and objectives and achieve a verifiably integrated architecture. This includes identifying, prioritizing, monitoring, analyzing, and reporting on the portfolio to satisfy the business requirements and supporting the Planning, Programming, Budget and Execution (PPBE) process.

The Contractor will assess portfolio alignment with DoD strategies, goals and objectives, provide capability performance measurement, provide portfolio risk assessment, and identify capability gaps, shortfalls and redundancies.

This work includes identifying and collecting decision-support requirements from the Directorates and working with the Architecture component to transform those requirements into architecture-informed Fit-for-Purpose views of the portfolio. These views will support ongoing PPBE-related activities.

Typical stakeholder activities include: Capability Gap Analysis, Capability Area Deep Dives, Issue identification, analysis and adjudication, budget estimates and assessments, redundancy identification, offset identification, and capability performance assessments.

The Army Portfolio Management System (APMS) is the primary tool. A USAFRICOM developed tool, AFRICOM Resource Integration Tool (AFRIT), is the secondary tool. However, others may be required to be used at any time.

C.6.2.5.2. System Administration Support

During this Task Order, it is anticipated that the Government may be need subject matter expert level systems administrators to support one or more of the tools listed below.

If exercised, the Contractor shall (consistent with the definitized requirements and technical direction issued by the Government):

a. Maintain hardware, inclusive of client and server systems; configure applications; apply security configurations and patches; upgrade applications or operating systems; or expand the functionality of supported application(s) for the suite of tools listed below.
b. Provide Tier 1 though Tier 3 support.
c. Support system and software prototyping initiatives to test, evaluate, and analyze potential information technology solutions.

The current tool suite (listed below) includes Windows Server, SharePoint, Microsoft Dynamics CRM, Microsoft SQL and Government owned proprietary software. However, support for other tools may be identified throughout performance if additional products are adopted by the Government in the future.

a. CaseWise EA tool application and repository.

b. EA SharePoint Site, custom SharePoint dashboard, webparts and backend database structures
c. Task Management Tool (TMT) application tool - a Microsoft Dynamics CRM based solution that facilitates communication, research, and responding to tasks efficiently and accurately.
d. System Integration Facility (SIF) - a VMWare based virtual network laboratory used to develop, prototype, test, evaluate, and stage systems and software.
e. AFRICOM Resource Integration Tool (AFRIT) - a custom asp.net and custom tool developed for budgeting and financial data.
f. Statistical Measurement And Reporting Tool (SMART) - a custom asp.net, java script, and custom coded assessment tool.
g. Enterprise Project Management Server (EPMS) - a custom configured instance of Microsoft Project Server with SharePoint integration.

C.6.3. EUCOM SPECIFIC OPTIONS

Options described in this section may be invoked to support EUCOM-related requirements.

C.6.3.1. KNOWLEDGE MANGEMENT (OPTIONAL)

During this Task Order, it is anticipated that the Government may require full-time Knowledge Management experts to be exercised at the Government's discretion. If exercised by the Government, the Contractor shall apply KM expertise to meet EUCOM objectives to improve collaborative information sharing and to support the EUCOM KM program's vision to continuously increase EUCOM's ability to collaborate, communicate, and act quicker and more effectively internally and among mission partners based on commander's intent, priorities, and objectives.

For proposal purposes, include an optional KM labor mix based up performance at Patch Barrack and the Contractor's CONUS Site(s). As a minimum, the KM Content Management SMEs shall be located at Patch Barracks. EUCOM seeks an optimal mix of on-site and off-site labor that provides the requisite skills to perform the work described in this section in a high quality, cost-effective manner. Historically, the EUCOM KM program has been supported by 23 FTE with current staffing level of approximately 20 FTE.

The Contractor shall, consistent with technical direction provided by the Government:

a. Provide KM expertise to manage and guide the EUCOM KM program. This includes:

(1) Providing advanced Business Process Engineering/Analysis and KM Expertise throughout the development of KM solutions.

i. Performing process analysis and modeling using industry-endorsed techniques (e.g. lean six sigma); employing related disciplines such as requirements analysis, outreach/engagement, quality communications, strategic/systems thinking, etc.

ii. Serving as strong, vocal proponents of KM around the headquarters and across the theater. Whenever advocacy, communications, or support is required, it is this role that will be engaged. In the past, such support was delivered in the form of directed engagement, informal training, support to both established and ad hoc teams, and even temporarily deployed contingency support.

(2) Providing advanced software and systems design and engineering expertise throughout the development of KM solutions.

i. Performing requirements analysis, planning, design, integration, implementation, testing, deployment, documentation, and sustainment.

ii. Applying expertise that encompasses software/hardware technologies employed at EUCOM which includes, but is not limited to the Microsoft family of software platforms (particularly Windows, SharePoint, Office Communications Server/LYNC, CRM, Exchange, SQL, Office, Silverlight, and Visual Studio), Google Earth, Adobe Connect, Jabber, and Telligent. Numerous complementary technologies are also employed.

iii. Complying with relevant EUCOM and higher strategies, policies, standards, and practices.

iv. Addressing interface/graphical design, database architecture, and enterprise systems integration requirements.

(3) Applying Principled Leadership to maintain, promote, and refine internal KM business practices at EUCOM. It should be noted that agile management principles are the cornerstone of internal KM business practices at EUCOM.

b. Provide KM expertise to satisfy INFORMATION DISCOVERY/SHARING requirements. This includes:

(1) Producing documentation and policies that promote KM best practices, such as:

i. Developing, updating and maintaining "Tactics, Techniques, and Procedures" and policies applicable to both the headquarters and theater to guide management and governance of the CIE.

ii. Making adjustments to existing procedures and policies (e.g. KM, unclassified information sharing, classification guidance, foreign disclosure, public release, operational reporting, etc.).

iii. Leveraging Furthermore, policies alone cannot shift culture – outreach, communications, incentives, etc. (coupled with training discussed below) must be leveraged to promote changes in behavior.

(2) Conducting analysis of information usage to elicit requirements, recommend possible courses of actions/solutions, and develop proactive information delivery solutions and techniques. Present concepts include Amazon-like information delivery leveraging search metrics and creation of a "My Site" sidebar that would increase availability of personal profile and portal-based storage.

(3) Manage, refine and mature EUCOM's metadata ontology. This includes maintaining all elements of the metadata ontology (terms, term store, taxonomy, application, supporting technologies, management processes, etc.) for the CIE to remain accurate and relevant.

(4) Responding to emergent information discovery/sharing requirements, providing solutions that offer the necessary agility to address the fluid nature of EUCOM operations. This work typically involves developing relatively simple solutions, followed by brief engagements with stakeholders. Requirements will be validated, scoped, and prioritized by the EUCOM KM leadership.

c. Provide KM expertise to satisfy DECISION SUPPORT requirements. This includes:

(1) Developing and enhancing the command's collaborative information environment (CIE). The portal is the most crucial aspect to the command's CIE and metadata and search represent the most crucial services in the portal. These services must be made progressively more mature in order to satisfy staff information requirements – the foundation of effective decision-making. Efforts in this area must be coordinated with the "Collaboration" tasks as information sharing is a social activity.

(2) Developing effective solutions to enhance the command's decision-making processes and increase the speed and accuracy of the decision-making. Solutions typically take the form of either dashboards (data visualization solutions) or improvement of a supporting process. Most requirements will be emergent in nature. Requirements will be validated, scoped, and prioritized by the EUCOM KM leadership.

d. Provide KM expertise to optimize COLLABORATION requirements. This includes:

(1) Developing an expertise locator solution (analogous to white/yellow pages) integrated with other social networking services, making use of current infrastructure/services (e.g. Active Directory, SharePoint Server, Office Communications Server, Joint Personnel Administrative Database (JPAD), etc.).

(2) Expanding federation of social networking services. Collaborative services must be connected to the enterprise to truly improve communications. Coordinate improvement with mission and technical partners.

(3) Promoting and institutionalizing the use of social networking/collaborative tools; assisting EUCOM with developing and implementing policy and practices that enable EUCOM to realize the value of effective internal and external social networking.

e. Provide KM expertise to optimize INFORMATION FLOW.

(1) Develop a corporately-maintained services catalog/help solution for the command. Related to the expertise locator, develop/implement a centralized services directory and related documentation repository for the command. The solution should be user-maintained.

(2) Improve operational information flow. Institute KM best practices and increase the quality of situational awareness/shared understanding at EUCOM through engagement with the EUCOM Mission Command Center (EMCC). This includes evaluating processes, formulating solutions, conducting training, and codifying results.

(3) Support coalition and partner information sharing to help overcome information flow difficulties when sharing with non-DOD partners. This includes analyzing requirements, capabilities, and policy to determine opportunities to improve performance in this area.

f. Provide KM expertise to support EDUCATION/TRAIN EUCOM staff on KM principles and practices. This includes implementing a robust KM training program that encompasses:

(1) Developing and delivering KM training to reach all newcomers and that continues to educate and train advanced practitioners/leaders.

(2) Developing and delivering collaborative tool training to increase staff proficiency with collaborative tools through implementation of a robust training program. Reach all newcomers and continue education and training for advanced practitioners/leaders.

(3) Facilitating relevant user groups and/or communities of interest to engage practitioners of KM and through hosting collaborative tools use sessions to increase the skills of the most advanced users and provide a forum for informing users about the program.

(4) Conducting strategic outreach, facilitating KM working groups, and assisting in the management of the KM governance process to support synchronization of KM initiatives with internal and external partners. This includes participating in key meetings of the command's staff and making recommendations in line with KM practices.

g. Provide KM expertise to support PROCESS IMPROVEMENT requirements. This includes:

(1) Developing a key/senior leader engagement management solution to provide a methodology and tools for planning and tracking engagements across the theater.

(2) Developing an integrated command calendar solution to improve EUCOM's capabilities for effectively coordinating and deconflicting events.

(3) Enhancing the command's lessons learned (LL) program; equipping EUCOM with improved observation collection techniques, LL management solutions, and lesson management/ remediation support.

(4) Completing the command's Requirements Management System (RMS) and Mature Corresponding Processes to enable the command to make well-informed decisions about requirements, to better-manage resources, and to support the deliberate requirements governance process. Two modules remain to be developed (contracts management and un-funded requirements).

(5) Refining the command's "country pages" to enable command staff and senior leaders to monitor activity across the AOR and improve situational awareness capabilities.

(6) Respond to emergent process improvement requirements to improve unforeseen process shortfalls/problems. Requirements will be validated, scoped, and prioritized by EUCOM KM leadership.

C.6.3.2. THREAT ASSESSMENT SERVICES (OPTIONAL)

During this Task Order, it is anticipated that the Government may require up to five (5) full-time cyber threat assessment experts to be exercised at the Government's discretion. If exercised by the Government, the Contractor shall apply threat assessment expertise to enhance EUCOM's existing cyber threat capabilities and to develop an enhanced Cyber Threat Detection and Defense capability for EUCOM and the EUCOM Theater. The scope of this support includes providing the resources (inclusive of labor, software, hardware, and data) to support the fusion of these cyber threat detection and defense capabilities in a way that provides advanced global threat analysis and resolution. This includes the development and enhancement of Roles and Responsibilities; Operating Procedures; Software Development, Integration, and Implementation; Training; and Analysis related to this capability.

For proposal purposes, include the following optional positions based on a 1,860 hour man-year in each year of performance:

Optional Support	No. FTE	Base Year	Option Year 1	Option Year 2	Option Year 3	Option Year 4
Threat assessment experts	5	9,300 Hours	9,300 Hours	9,300 Hours	9,300 Hours	9,300 Hours

It is expected that Contractor personnel will require:

- Top Secret / Sensitive Compartmented Information (TC/SCI) clearance
- IAT Level II (GSEC, Security+, SCNP or SSCP) and CND Analyst (GCIA) certifications to be compliant with DoD 8570.01-M.

If exercised, the Contractor shall, consistent with technical direction provided by the Government:

a. Assist in the enhancement of EUCOM's existing Cyber capabilities. This includes:

(1) Implementing new organizational and reporting structures as defined by the Government.

(2) Providing correlation and analysis of threats and risks across HQ EUCOM internal/external public/open source data.
(3) Identifying hostile threat methodologies, attack vectors, and activity of interest.
(4) Providing focused operations/threat analysis on known intrusion sets (including but not limited to identifying new attack methods and vulnerabilities exploited).
(5) Discovering, tracking, reporting, and fusing global network events of interest utilizing cyber intelligence analysis data and methods.

b. Support training and knowledge transfer requirements by delivering training on Cyber threat topics and situation and conducting knowledge transfer on Cyber related topics.

c. Apply Cyber Subject Matter Expertise (SME) in adversarial methodologies in the Cyber domain and participate in Operational Planning Teams (OPTs).

The Contractor shall make recommendations for implementing changes so that EUCOM and Theater human and technical resources are combined, creating an enhanced cross-functional, cross-organizational Cyber Threat Analysis capability, thereby improving the defensive posture of the Theater.

Specific deliverables associated with the optional support are expected to include:

a. **WEEKLY REPORTS -** The Contractor shall provide weekly Tip/Threat Summary Reports via email (NIPR, SIPR and/or JWICS) every Friday on world-wide cyber threat occurrences and trends that may affect Blue Force networks in the EUCOM Theater.

b. **CYBER TIPPERS -** The Contractor shall provide cyber tippers as required for any cyber events that could impact Blue Force networks in EUCOM Theater.

c. **BRIEFINGS -** The Contractor shall provide briefings and reports as needed to various entities in the Cyber Center, JFCCC and EUCOM HQ based on intrusions, events or world-wide actions that could impact Cyber in the EUCOM Theater.

d. **NETWORK INTELLIGENCE REPORTS -** The Contractor shall create Network Intelligence Reports on large intrusions or events that affect multiple Blue Force Networks in the EUCOM Theater.

e. **AD HOC REPORTS -** The Contractor shall provide briefs for leadership that will be created as requested by the Cyber Center, JFCCC and/or EUCOM HQ to educate leadership on events, intrusions and actions taking place in the Cyber Domain.

f. **SPOT REPORTS -** The Contractor shall provide spot Reports on intrusions and events that occurred in the EUCOM Theater and need a quick turnaround in an effort to provide information in a serialized manner to various Cyber communities.

C.6.4. CAMP LEMONNIER - DJIBOUTI SPECIFIC OPTIONS

Options described in this section may be invoked to support Camp Lemonnier - Djibouti -related requirements, both on-site and remotely.

C.6.4.1. ENGINEERING AND IMPLEMENTATION (OPTIONAL)

During this Task Order, it is anticipated that the Government may require optional services to engineer and implement technical solutions specific to fulfilling unique needs at Camp Lemonnier – Djibouti. Specific requirements will be definitized at the point of exercising an option.

For proposal purposes, include the following optional positions in each year of performance based on a 2,880 hour man-year at CLDJ-HOA and a 1,000 hour man-year for the Project Manager position:

Optional Support	No. FTE	Base Year	Option Year 1	Option Year 2	Option Year 3	Option Year 4
a. Sr. Systems Engineers -- **This position must be on-site**	3	8640 total hours	8640 total hours	8640 total hours	8640 total hours	8640 total hours
b. Project Manager -- **This position does not have to be an on-site resource**	1	1000 hours	1000 hours	1000 hours	1000 hours	1000 hours

The scope of this support includes providing the staff and resources necessary to support the planning, design, and implementation of changes associated with AFRICOM operations on the JEN in both the NIPR and SIPR environments. Contractor services include planning and engineering actions providing draft documentation and technical input to documentation for assessments, plans, system implementations and architectures, and engineering designs related to the evolving AFRICOM enterprise.

If exercised, the Contractor shall, consistent with the definitized requirements:

- Provide emerging communications and information technology engineering support and technical solutions to improve customer service, system performance, and reliability.
- Provide C4 Network technical support.
- Test and evaluate commercial-off-the-shelf applications for integration into the C4 networks.
- Participate in planning activities.
- Provide feedback to both short-range and long-range planning activities to enhance performance and improve efficiency.
- Provide effective technical solutions to complex problems.
- Provide technical information, analysis, and recommendations for information technology, C4 issues, and systems.
- Provide network design and engineering support to include designing and engineering configurations for new network installations and upgrades. Integrate hardware, software, computer projection systems, video switching hardware, video teleconferencing, and other systems to meet the requirements.
- Provide technical studies, review plans, evaluate state of the infrastructure in order to field and integrate new systems and/or equipment within the proposed timelines.
- Provide security analysis and security design review in order to recommend fielding and integrating new systems and/or equipment.
- Review C4 plans/policies and provide observations/questions for consolidated responses.
- Provide technical analyses and draft reports of C4 system tests, assessments, and architectures to include remote management of the enterprise using AFRICOM selected tools.
- Implement and integrate systems and approved engineering designs as required to support AFRICOM JEN operations.

C.6.4.2. SHAREPOINT DEVELOPMENT (OPTIONAL)

During this Task Order, it is anticipated that the Government may require optional services to develop and enhance Sharepoint solutions.

For proposal purposes, include the following optional positions in each year of performance based on a 2,880 hour man-year at CLDJ-HOA and a 1,860 hour man-year for remote positions:

Optional Support	No. FTE	Base Year	Option Year 1	Option Year 2	Option Year 3	Option Year 4
a. CLDJ-HOA On-site Sharepoint Professional	1	2880 hours	2880 hours	2880 hours	2880 hours	2800 hours
b. Remote Sharepoint Professional	1	1860 hours	1860 hours	1860 hours	1860 hours	1860 hours

AFRICOM has designated the JEN-HOA SharePoint portal as the gateway for staff and organizational processes within the Horn of Africa region. Contracted developmental support of the AFRICOM portal on the NIPRNET and SIPRNET allows initial operating capability (IOC) functions to mature across the command. Some of these capabilities include, but are not limited to: electronic staffing; calendar management, task management, and dashboard/business intelligence (BI) visualization development. The JITSMO-HOA SharePoint Portal Team provides SharePoint support to all of Combined Joint Task Force – Horn of Africa (CJTF-HOA), including all Forward Operating Locations (FOLs) and all other tenant organizations on CLDJ.

If exercised, the Contractor shall provide technically proficient Sharepoint professional(s) to assist AFRICOM in analyzing the current portal capabilities; and shall provide expertise in optimizing those capabilities and executing tasks based on command guidance and consistent with definitized technical requirements provided at the time of option exercise. Requirements will be validated, scoped, and prioritized by the TPOC. The scope of this support includes but is not limited to the following areas:

- Defense Enterprise Portal Service (DEPS) customization,
- portal migration,
- REL portal development,
- Tasker management,
- Dashboard/business intelligence visualization development,
- Calendar management,
- Content management,
- Electronic staffing and expertise locating services.

Measures of success include meeting Department of Defense information assurance (IA) parameters and adhering to DISA Security Technical Implementation Guidelines (STIG). The tasks shall be completed by the due dates specified for each task as determined by the Government approved in a detailed action plan.

C.6.4.3. HOST BASED SECURITY SYSTEM (HBSS) SUPPORT (OPTIONAL)

During this Task Order, it is anticipated that the Government may require optional services to provide Host Based Security System support.

For proposal purposes, include the following optional positions in each year of performance based on a 2,880 hour man-year at CLDJ-HOA:

Optional Support	No. FTE	Base Year	Option Year 1	Option Year 2	Option Year 3	Option Year 4

CLDJ-HOA On-site HBSS position	1	2880 Hours	2880 Hours	2880 Hours	2880 Hours	2880 Hours

The Host Based Security System (HBSS) solution suite is an enterprise-wide automated, standardized tool that provides host-based security, against both insider threats and external threats. DISA, at the request USSTRATCOM and in support of National Security goals established by the President; purchased from industry, a capability that will develop and deploy an automated HBSS solution. HBSS supports the "Defense-in-Depth" initiative by providing network administrators and security personnel with mechanisms to prevent, detect, track, report, and remediate malicious computer-related activities and incidents across all DoD networks and information systems throughout the DoD Enterprise.

If exercised, the Contractor shall, consistent with technical direction provided by the Government:

- Monitor and ensure the security health of the workstations and servers protected by the Host Based Security System (HBSS) product suite.
- Ensure all HBSS components are online, communicating and are at current versions.
- Lead the HBSS Event Analysis, HIPS tuning and incident response process.
- Validate unknown behavior with appropriate functional group through ePO or HBSS Analysis and HIPS Tuning Tool.
- Research all available information to identify if a system is under attack or a component is not functioning correctly.
- Provide regular reports to IA management team to maintain situational awareness.
- Ensure anti-virus definitions are updated and that local security policies are enforced; unmanaged hosts are tracked and remediated; evaluate and mitigate any discrepancies.
- Ensure the installation and support of HBSS meets all US Cyber Command and DOD requirements and timelines as identified in FRAGO 13 or applicable OPORDs/TASKORDs.
- Adhere to guidance contained in the current DISA HBSS Tier 3 Operations Tactics, Techniques and Procedures documentation.

C.6.4.4. INSIDE PLANT (ISP)/PROTECTIVE DISTRIBUTION SYSTEM (PDS) ENGINEERING AND INSTALLATION (OPTIONAL)

During this Task Order, it is anticipated that the Government may require optional engineering and installation services to support the build-out of identified facilities with requisite communications and IT infrastructure.

For proposal purposes, include five (5) optional FTE positions based on a 2,880 hour man-year on-site at CLDJ-HOA in each year of performance.

If exercised, the Contractor shall, consistent with the definitized requirements provide:

a. **Passive Infrastructure Design and Installation Services**. The Contractor shall install, remove, modify, and maintain passive infrastructure inside existing or newly constructed/remodeled buildings. Such passive infrastructure may include, but not be limited to simple distribution system, protected distribution system (e.g. alarmed, etc), raceway and/or stack connectivity between floors and communications closets, air-gap boxes and similar devices, patch panels and similar devices, and all other forms of connectivity (regardless of media type) not directly connected to a power source.

The Contractor shall install, remove, modify, and maintain communications and IT end user devices inside existing or newly constructed/remodeled buildings. Such communications and IT end user devices may include, but not be limited to alarmed carrier components, desktop computers, monitors, multi-system switching devices, desktop VTC, scanners, printers, telephones (analog and digital), secure telephone equipment (STE), and all other end user devices connected in some way to a form of communications or IT network.

The Contractor shall perform network drop additions, moves, and removals. The Contractor shall acquire, install and integrate all components necessary to implement an Internal Cable Distribution and Protected Distribution System (PDS) to support NIPR and SIPR network access in accordance with the requirements set forth in this PWS. The Contractor shall supply all material and labor to install, integrate, test and make NIPR and SIPR passive infrastructure operational, minus the active infrastructure. The Contractor shall provide a site survey, on/off site engineering, Bill of Materials (BOM) identification and procurement, site preparation, installation, verification testing and quality control for all internal NIPR and SIPR passive infrastructure projects/service requests approved by the COR.

This work is expected to include projects ranging from temporary facilities (i.e. tents) to Containerized Work Unit(s) to hardened facilities and may include communication rooms and/or server rooms. The work may include anything from adding infrastructure to existing facilities to renovation of facilities to new construction. Projects will be classified into Type A or Type B based upon the recommendation of the Contractor and concurrence of the Government.

- Type A projects generally are smaller projects which could include tents, CWUs, or a few rooms within a hardened facility.
- Type B projects generally are larger in scale normally include new construction and major renovation of harden facilities but could also include multiple CWUs or tents.

It is anticipated that a continuous on-site presence will be required to work Type A projects as many are short notice. It is anticipated that on-site support could be supplemented (with prior Government approval) with TDY personnel to work the Type B projects by leveraging surge under PWS section 6.6. The Government will ensure Type A projects are scheduled such that the actual ISP work will not over tax the on-site ISP team unless allowances are made for additional manpower resources.

b. **Physical Plant Configuration Management Services.** AFRICOM leverages a comprehensive Configuration Management System (CMS) that consolidates the IT physical plant and supporting passive infrastructure/connectivity data in one repository. The intent of the CMS is to provide for centralized management across various regions of the physical plant, thereby streamlining physical plant maintenance; reducing operational management costs and leveraging Critical Infrastructure Information to aid in identifying service faults and expedite troubleshooting. The CMS incorporates Inside Plant, Outside Plant, Data Center, WAN, Cable, and Circuit management in one place, providing AFRICOM with the oversight necessary to maintain critical operations. The CMS brings together data normally kept in disparate spreadsheet, CAD, and home-grown database files to create a more complete visual picture of an enterprise IT network environment.

The Contractor shall use the AFRICOM CMS to document, manage and track Critical Infrastructure Physical Plant Management data for the Inside Plant, Data Center, and Wide Area Network. The Contractor shall use the CMS to provide the following support:

- Physically trace end to end transmission paths throughout the local network
- Highlight physical circuit traces and actual routing in order to visualize redundancy and physical separation of mission-critical services
- Manage data center equipment rack elevations
- Manage data center Multi-Tiered Space/Floor plans
- Provide multi-dimensional data center power management

C.6.4.5. CONTINGENCY IT SYSTEMS SUPPORT (OPTIONAL)

During this Task Order, it is anticipated that the Government may require optional support to provide enhanced IT systems engineering, operations and integration support for additional C4 mission areas in order to meet emerging contingency requirements within the AFRICOM Theater of Operations.

For proposal purposes, include the following optional hours based on a 2,880 hour man-year in each year of performance providing on-site support at Camp Lemonnier, Djibouti and deploying (where specified during performance) to Forward Operating Locations throughout the Combined Joint Operations Area of East Africa:

Optional Support	No. FTE	Base Year	Option Year 1	Option Year 2	Option Year 3	Option Year 4
Sr. Systems Administrator	2	5760 hours	5760 hours	5760 hours	5760 hours	5760 hours
Sr. Systems Engineer	1	2880 hours	2880 hours	2880 hours	2880 hours	2880 hours

a. **Global Command and Control System (GCCS) Support.** The GCCS Support personnel shall support the Commander, Combined Joint Task Force – Horn of Africa (CJTF-HOA) by operating, administering and maintaining the Global Command and Control System - Joint (GCCS-J). GCCS-J is a state-of-the-art, event-driven, computer system which features comprehensive command and control applications connected to the SIPRNET, and other networks, supporting staff, action officers, Joint Task Forces and subordinate commands in Germany, Africa and elsewhere in AFRICOM.

The Contractor shall provide systems administration support for the GCCS systems. Through proper system administration and system monitoring, the Contractor shall ensure the GCCS systems are available and operating efficiently. In support of this contract, the Contractor shall provide on-site system administration support and installation/configuration - or assist with installation and configuration of GCCS servers and clients in Djibouti and at supported sites.

The Contractor shall recommend and evaluate Commercial-Off-The-Shelf (COTS) products or unique solutions (scripts, business practice re-engineering) to streamline system administration and/or user access to GCCS systems. The Contractor shall provide troubleshooting of system problems and make recommendations for problem resolution.

b. **CJTF-HOA Expeditionary C4 Support.** The Combined Joint Task Force – Horn of Africa (CJTF-HOA), and its associated units, is located at Camp Lemonnier, Djibouti with various Forward Operating Locations throughout the Combined Joint Operations Area of East Africa. CJTF-HOA is a sub-unified command of AFRICOM. However, unlike with other sub-unified commands, AFRICOM has agreed to provide standard core communications and IT support for them as if they were standing elements of the COCOM's Headquarters staff (e.g., Directorate-level).

As such, core communications and IT O&M support is provided specifically for these CJTF-HOA personnel assigned to and working day-to-day at the CJTF-HOA Headquarters and also for sub-elements or personnel deployed downrange. The CJTF-HOA J6 Directorate (CJ6) supports C4 efforts for joint and combined operations in the CJTF-HOA AOR.

CJ6 plans, installs, operates, maintains and supports secure, reliable, redundant and robust command and control tactical communications for CJTF-HOA staff and forward-deployed units within the Combined Joint Operations Area.

The scope of this optional support includes providing expanded IT support for all expeditionary/tactical communications related to CJTF-HOA and any other IT support not directly tied to existing baseline services provided as part of the applicable AFRICOM C4IM Services Catalog.

Existing network architecture diagrams and associated hardware/software lists will further define the tactical/expeditionary network as appropriate. The tactical network is currently treated as an interconnected information system within the AFRICOM Joint Enterprise Network accreditation boundary. Further, problems may range from the simple to the complex and require a broad knowledge and understanding of the various types of data network hardware, software, and systems to include how they interface with each other. The scope of this support includes deploying contractor personnel down-range. This support may span other requirements described in previous PWS sections or as identified in technical direction provided by the COR.

C.6.5. SOCEUR/SOCAF SUPPORT (OPTIONAL)

Special Operations Command Europe (SOCEUR) and Special Operations Command Africa (SOCAF) act as sub-unified commands of EUCOM/AFRICOM. However, unlike with other sub-unified commands, both EUCOM and AFRICOM have agreed to provide standard core communications and IT support for them as if they were standing elements of the COCOM's Headquarters staff (e.g., Directorate-level). As such, core communications and IT O&M support, if exercised, would be provided specifically for those SOCEUR/SOCAF personnel assigned to and working day-to-day at the COCOM Headquarters, and not for sub-elements or personnel deployed downrange.

For proposal purposes, include the following optional labor mix based on a 1,860 hour man-year in each year of performance:

Optional Support
• Network Administrator, Senior
• Network Administrator, Journeyman
• Systems Administrator, Senior
• Systems Administrator, Journeyman

The scope of this optional support includes providing in Garrison Tier 1 basic helpdesk support, Tier 2, and standard Tier 3 Desktop/Touch maintenance support for the SOCEUR and/or SOCAF command personnel consistent with the scope described in PWS section 5.3 CUSTOMER SUPPORT. Problems may range from the simple to the complex and require a broad knowledge and understanding of the various types of data network hardware, software, and systems to include how they interface with each other. The scope is limited to providing in garrison support. Down-range support and deployment of contractors is outside the scope of this requirement. The primary focus of this support is expected to include:

- Providing dedicated 8 x 5 desktop support personnel to the SOCEUR and SOCAFRICA
- Desktop support for users regarding their services, applications and hardware;
- Touch Maintenance;
- Attending meetings and providing technical input as requested by the SOCEUR/ SOCAF;
- Providing VIP level support, where directed by the Government;
- Provide VTC MCU access for clients and server-server connections to SOCEUR and SOCAFRICA Voice and Video Environments (VVE);
- Managing network and cryptographic equipment;
- Providing management, engineering, analytical, technical support and integration services to special projects, consistent with technical direction provided by the GSA COR and the scope of requirements described in PWS C.5 TASKS. Evaluating emerging technologies as it relates to these special projects; and
- Supporting procurement of Tools consistent with Section H.2.4 TOOLS-HARDWARE/SOFTWARE and MISCELLANEOUS ODCs.

This support may span other requirements described in PWS section C.5 REQUIRED TASKS, as identified in technical direction provided by the COR.

Responding to end user requests for assistance in keeping systems operational shall be expeditiously handled; consistent with response times defined at the time that this support is exercised. The Contractor shall log all end user requests for assistance received, whether the problem was resolved, and the resolution. The log information showing support provided to SOCEUR/SOCAF end users shall be submitted to the COR as a part of the Monthly Status Report. Where recurrent problems are encountered, the Contractor may be requested to prepare instructions documenting steps to prevent or resolve such issues. This documentation shall be forwarded to the COR. Maintenance Log information for SOCEUR/SOCAF maintenance actions shall also be submitted to the COR as part of the Monthly Status Report.

C.6.6. GOVERNMENT DIRECTED OVERTIME/SURGE (OPTIONAL)

During this Task Order, it is anticipated that the Government may require the Contractor to work overtime or surge resources to support additional Government requirements while continuing to provide standard contracted services. It should be noted that optional government directed overtime or surge may apply to any mandatory tasks or exercised options under Section C of this Task Order.

For proposal purposes, the Not-to-Exceed (NTE) value of this option is $750,000 per year.

Typical examples of overtime support that could be exercised includes but is not limited to:

- Exercise support when adjusting the normal work schedule; minimizing/prohibiting leave of individual contractor employees; adjusting service level agreements DOES NOT achieve the required coverage.

- Real World Operations when adjusting the normal work schedule; minimizing/prohibiting leave of individual contractor employees; adjusting service level agreements DOES NOT achieve the required coverage.
- Crashing project schedule(s) to achieve Government directed completion dates.

Government directed overtime should only be used when all other possibilities have been exhausted. It should not be used to support normal O&M such as outages requiring Contractor employees to work after hours or weekends. Overtime costs shall <u>not</u> be incurred unless authorized by the Contracting Officer (CO) or the Contracting Officer's Representative (COR) and unless funding is available to cover incurred expenses.

At the time of exercising this optional support, at a minimum the Government will:

- Identify the event (exercise/operation/project) which is driving the overtime requirement
- Identify the specific services where overtime or surge is authorized
- Define level of effort expectations (i.e. 12-hour days, 6 days per week)
- Identify duration or end date when overtime is no longer required
- Provide an estimate on the number of overtime or surge hours required.

(END OF SECTION C)